

**Awareness and Perception of Phishing variants from Policing, Computing
and Criminology students in Canterbury Christ Church University**

By: Nima Movassagh

Canterbury Christ Church University

**Thesis submitted
for the degree of
MSc by Research in Policing**

Year: 2021

Abstract

This study focuses on gauging awareness of different phishing communication students in the School of Law, Policing and Social Sciences and the School of Engineering, Technology and Design in Canterbury Christ Church University and their perception of different phishing variants. There is an exploration of the underlying factors in which students fall victim to different types of phishing attacks from questionnaires and a focus group. The students' perception of different types of phishing variants was varied from the focus group and anonymised questionnaires. A total of 177 respondents participated in anonymised questionnaires in the study. Students were asked a mixture of scenario-based questions on different phishing attacks, their awareness levels of security tools that can be used against some phishing variants, and if they received any phishing emails in the past. Additionally, 6 computing students in a focus group discussed different types of phishing attacks and recommended potential security countermeasures against them. The vulnerabilities and issues of anti-phishing software, firewalls, and internet browsers that have security toolbars are explained in the study against different types of phishing attacks.

The focus group was with computing students and their knowledge about certain phishing variants was limited. The discussion within the focus group was gauging the computing students' understanding and awareness of phishing variants. The questionnaire data collection sample was with first year criminology and final year policing students which may have influenced the results of the questionnaire in terms of their understanding, security countermeasures, and how they identify certain phishing variants. The anonymised questionnaire awareness levels on different types of phishing fluctuated in terms of lack of awareness on certain phishing variants. Some criminology and policing students either did not know about phishing variants or had limited knowledge about different types of phishing communication, security countermeasures, the identifying features of a phishing message, and the precautions they should take against phishing variants from fraudsters.

Acknowledgements

I would like to extend my deepest gratitude to my family for all their support throughout my MSc by Research in Policing course. I would not be where I am if it wasn't for their guidance.

I would like to say thank you to my Canterbury Christ Church University research supervisors' Doctor Paul Stephens and Professor Steve Tong in the School of Law, Policing and Social Sciences at Canterbury Christ Church University for all of their support and guidance when writing this thesis.

Abbreviations

EC3-Europol's European Cybercrime Centre

IOCTA- Internet Organised Crime Threat Assessment

NCA- National Crime Agency

NCSC- National Cyber Security Centre

GCHQ- Government Communications Headquarters

MPS- Metropolitan Police Service

CLP- City of London Police

FBI- Federal Bureau of Investigation

FCA- Financial Conduct Authority

SFO- Serious Fraud Office

VPN- Virtual Private Network

SDN- Software Defined Networking

DPI-Deep Packet Inspection

GENI- Global Environment for Network Innovation

WHO- World Health Organisation

C and C Server-Command and Control Server

NFA- National Fraud Authority

GDPR- General Data Protection Regulation

VoIP- Voice Over IP

SMS- Short Message Service

NFIB- National Fraud Intelligence Bureau

URL- Uniform Resource Locator

https- Hypertext Transfer Protocol Secure

http- Hypertext Transfer Protocol

TOR/Tor-The onion router

CAPQ- Computer-based Anti-Phishing Questionnaire

JCAT-Joint Cybercrime Action Taskforce

ISPS- Internet Service Providers

GENI- Global Environment for Network Innovation

IoCs- Indicators of Compromise

AIS- Artificial Immune Systems

COVID-19- Coronavirus

UK- United Kingdom

IP Address- Internet Protocol Address

ICO- Information Commissioner's Office

APK- Android Package Kit

CNN- Convolutional Neural Networks

DDoS Attacks- Distributed Denial of Service Attacks

EMPACT- European Multidisciplinary Platform Against Criminal Threats

EU- European Union

TLD- Top-Level Domain

OTLD- Onion Top-Level Domain

CCTLD- Country Code Top-Level Domain

HW- Hidden Wiki

ASEAN- Association of Southeast Asian Nations

ASEANPOL- National Police Organisation for Association of Southeast Asian Nations

CNN- Convolutional Neural Networks

APWG- Anti-Phishing Working Group

CFC- Cyber Fusion Centre

RATs- Remote access tools

APT- Advanced Persistent Threat

NFATs- Network forensic analysis flow exporter tools

RNN- Recurrent Neural Network

NLP- Natural Language Processing

AI- Artificial intelligence

Glossary

The Onion Router Application (Tor which is also written as TOR) is used to access Dark Web. onion sites anonymising a user or a number of users when they visit. onion sites or a. onion site on the Dark Web. The name Tor is an abbreviation for The Onion Router. Tor is a software used for anonymised and encrypted communication on the Dark Web. Tor traffic passes through 7,000 relays which hides the location of a user. Tor network purpose is to protect user privacy (Islam and Ozkaya 2019).

Deep Web- The Deep Web (also known as the Undernet, hidden Web or invisible net consists of data which is not located by search engines.

Dark Web/Dark Net- is a subset of the deep web which include dark net .onion sites. Dark web sites mostly used for illegal criminal and terrorist activities. Dark web websites are not indexed by search engines. The dark web is only accessed through special browsers such is the Tor browser (Islam and Ozkaya 2019).

Smishing (Texts messages which are sent by fraudsters similar to a phishing email but can include a link to a malicious phishing website to steal information or download malware onto an electronic device).

Encryption is a process of converting data/information into code which can prevent unauthorised access from a third party. The purpose of encryption is to convert electronic data to unrecognisable or to an unreadable encrypted form which cannot be easily understood or read by third parties/ or from an individual.

Spyware- Software which enables a user to gain covert information about another person's computer activities by transmitting data covertly from their hard drive. The purpose of spyware is to send information to a third party.

Viruses- A piece of malicious code which is able to copy itself and typically has a detrimental effect, such as corrupting a system or destroying data. A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

Trojan Horses- A trojan horse might typically pose itself as or is embedded, in a legitimate programme, but it is designed for malicious purposes, such as: theft of data, deleting files, expanding an existing malicious botnet, spying, and carrying out DDoS attacks.

Virtual Private Networks (VPNs) encrypt traffic when a user connects to the internet. A VPN that blocks untrustworthy networks in between which may be challenging for law enforcement forces to trace cybercriminals. VPN may make it difficult for digital forensics employees to investigate online fraud (Aragues, 2017).

Remote Access Trojan otherwise known as (RAT)- Gains access to a computer system or mobile device remotely. A (RAT) may be installed by hackers using a piece of malware. This could give them total control to the attacker, who can use it to carry out a variety of actions: executing malicious commands, logging keystrokes, taking screen shots, sending files and documents to the attacker and monitoring actions.

Computer Worms-A worm can be used to replicate itself over a computer network and performs malicious actions without guidance.

Keyloggers: Keystroke logging is an act in which tracking and recording of every keystroke entry made on a computer, often without the permission or knowledge of the user. Keyloggers might be used in software based or hardware based as a legitimate personal or professional IT monitoring tool. Keystroke logging can be used for criminal purposes. For example, keystroke logging is used as malicious spyware that may be used to capture private information like passwords or financial information which may be sent to third parties for criminal activities and exploitation.

Rootkit- A rootkit is used to collect information by using different programmes that allow administrator-level to a computer network or a computer. This can allow the attacker to be granted privileged access to the computer or gain root and possibly deploy malicious activities on other machines in the same network or networks.

Cybercrime- Cybercrime is a fast-paced type of transnational crime which affects INTERPOL's and Europol's member countries as well as different police forces across England and Wales. The growth in cases of cybercrime is because of the internet and computer technology which has enabled economic and social growth reliance on the internet. This has led to different vulnerabilities and threats from criminal activities. For example: *'The Global Cybercrime Strategy outlines INTERPOL's plan to support member country efforts to combat cybercrime by coordinating and delivering specialised policing capabilities from 2016 to 2020.'*

APT (Advanced Persistent Threat)- APT uses sophisticated hacking techniques to access a system. An APT threat is stealthy threat actors who may be nation-state or state-sponsored groups.

Botnet- A botnet is when numerous internet-connected devices which are used to run one or multiple bots. Botnets can be used to carry out criminal activities such as to perform Distributed Denial-of-Service (DDoS) attacks, steal private information, distribute spam, and enable hackers to access devices and its connection. The owner of a botnet can control the botnet and feed it commands using a command and control (C&C) software. The word botnet means 'robot' and 'network'. The term might be associated with negative or malicious connotations by some people (Thingbots, 2016).

Peer-to Peer Botnet- Peer-to-Peer Botnet is used to detect and terminate IRC botnets, bot owners might deploy malware on peer-to-peer networks. These bots might use digital signatures so thus only someone with access to the private key can control the botnet (Heron, 2007).

Malware- This is an abbreviated term which means 'malicious software'. This is software which is designed to gain access or damage a computer without the knowledge of a user. There are malware variants which include: keyloggers, viruses, spyware, worms or other types of malicious code that breaches a computer (Norton, 2020). Malware purpose is to hijack computer networks or systems in order to carry out the theft of private information from a device or devices. Malware has different names such as: viruses, adware, spyware, keyloggers and so on. Malware can be distributed by phishing variants, USB and external hard drive.

Interpol- Their full name is the International Criminal Police Organisation, and they work with inter-governmental organisation. They have 194 member countries and help police to make the world a safer place (Interpol, 2020).

Europol- European Union's law enforcement agency. Their main goal is to ensure Europe is safer for everyone and benefit EU citizens. Europol investigate organised fraud, international drug trafficking and money laundering, trafficking in human beings and terrorism.

FBI- Federal Bureau of Investigation (FBI) is a domestic intelligence and security service. They investigate cybercrime, money laundering, drug trafficking, cyber-terrorism, terrorism and so on. They may work collaboratively with other law enforcement agencies such as: Interpol and Europol.

Phishing- Phishing is when hackers attempt to gain person information using malicious e-mails and phishing sites. Some phishing variants such as: Vishing, Smishing and Spear-Phishing are becoming increasingly sophisticated form of cyber-attack.

Spear Phishing- Spear Phishing is a variant of phishing in which hackers send emails to a specific group of people with common characteristics or other identifies. Spear Phishing Emails appear to originate from a or trusted source such as a Europol police recruitment email applied previously by an individual. Hackers use spear phishing to harvest classified information or personal information from a victim or group of victims depending on the success rate of a spear phishing email sent by hackers.

Honeypot- A honeypot is a term used when a computer system is intended to attract cyberattacks (like a decoy). It stimulates a target for hackers to exploit and use their intrusion attempts to gain intelligence from them and cyber-forensic experts could possibly find the source of the attacks launched by them (Kaspersky, 2020).

WI-FI- is protected access (WPA) is a security protocol used within wi-fi networks. This is significant improvement on WEP because it can offer a higher level of protection through more sophisticated data encryption.

Server- A server is a computer which can handle requests for email, data, file transfers and other network services from other computers.

Address- Identifies the location of an internet resource. This will mean that if an email address is linked to an address, a web address (http:// or https:// or an internet address (000.111.011.0)).

Browser- A program used to access World Wide Web pages. For example: Safari, Google Chrome, Firefox or Internet Explorer. Some browsers such as the Tor browser is used to access dark nets or deep web sites (Islam and Ozkaya 2019).

Polymorphic malware- Polymorphic malware is a malware variant that changes on a regular basis in order to avoid detection. The majority forms of malware can be polymorphic including worms, bots, viruses, trojans or keyloggers.

Metamorphic virus- This malware variant is able to change its code and signature patterns with each iteration. Metamorphic viruses are more advanced in comparison to polymorphic viruses.

Software Defined Networking- Software Defined Networking (SDN) is a network architecture approach. It allows a network to be controlled or programmed using software applications. It can help operators to manage an entire network regularly and holistically. SDN separates a data plane from a control plane in routers and switches (Ciena, 2021).

Deep Packet Inspection- Deep packet inspection (DPI) is used to examine and manage network traffic. DPI is a type of packet filtering that identifies, locates, classifies, reroutes or blocks packets with specific data or code payloads (Scarpatti, 2017).

Adaptive Dynamic Spiking Neural Network algorithm- Spiking neural networks can exploit the network dynamics for learning. For example, synchronisation spike trains can allow the user to decode the network outputs from the synchronisation patterns (Romera and Talatchian, 2018). Adaptive Dynamic Spiking Neural Network algorithm have classification capabilities of spiking networks which are trained used to unsupervised learning methods (Ponulak and Kasinski, 2010).

Network forensic analysis flow exporter tools (NFATs)- are used to monitor anomalous traffic to perform forensic analysis. The tools are used to get an insight of their environment. They are designed to gather evidence on the network and capture packets to gather evidence and analysis of data (Sira, 2003).

Script Kiddie- Script kiddies use software or scripts written by others and do not have the knowledge or know how to modify or produce their own software (HYPR, 2021).

Elite hacker- is the name used to identify those individuals who think they are experts in their line of work (SecPoint, 2021).

Recurrent Neural Network- A recurrent neural network (RNN) is an artificial network. RNN can be in speech recognition and natural language processing (NLP). RNNs created to analyse data's sequential characteristics and use patterns to predict a scenario (Laskowski, 2018).

Deep Neural Network- A deep neural network is a neural network to process data in complex ways. Deep neural network is a type of machine learning when the system uses artificial intelligence to classify and order information (Techopedia, 2021).

Adam Optimizer- Adam is an algorithm used for stochastic gradient descent for training deep learning models (Brownlee, 2017).

Stochastic- Stochastic is a machine learning process when the outcome is unpredictable. In a stochastic process, each event is random. A stochastic process has a hidden pattern that connects each of these events found from a stochastic process. A stochastic process decodes hidden patterns. At the end of the stochastic process, predication made from the decoded data (Ippolito, 2019).

Artificial intelligence- AI-based technologies are for cyber defence. However, AI can automate cyberattacks. For example, to send phishing communication attacks to people (Yamin et al., 2021).

Contents Page

Abstract –2

Acknowledgements- 3

Abbreviations- 4-7

Glossary- 8-13

Introduction- 16

Background Research- 17-42

Methodology- 43-59

Results- 60-97

Conclusion- 97-104

Bibliography-105-151

Appendix-152-191

Ethics Approval Letter- 153

Data Protection Act (2018) and GDPR (2016) compliance in the study-154

Consent Details-155-157

Participant Information Sheet-158

Confidentiality-157

Questionnaire-159-166

Introduction

This study will be looking at the awareness levels of Canterbury Christ Church University students who are studying an undergraduate degree course in Policing Criminology and Computing and assessing their knowledge and awareness on different types of phishing attacks. There will be a focus group with computing students who will be asked open-ended questions about certain phishing attacks from some students. Also, the anonymised questionnaires will be assessing the knowledge and awareness from students on different types of phishing communication. The study will be using a mixed methodology of anonymised questionnaires and a focus group. The anonymised data from the questionnaires and the focus group will be analysed in order to find areas the students' knowledge is weakest about certain phishing variants.

The study focuses on gauging awareness levels of phishing emails from students studying policing, computing and criminology at Canterbury Christ Church University and their perception of different types of phishing email and their variants with the goal of comprehensively answering the following research questions:

Research Question 1: *What are the underlying factors in which students fall victim to different types of phishing attacks?*

Research Question 2: *Does the perception of different types of phishing emails from students correspond with statistical information in a focus group and anonymised questionnaires?*

This study aims to determine if there is a knowledge gap from undergraduate students and their understanding of different types of phishing attacks. Once, the lack of awareness of phishing variants have been identified in the study there will be recommendations made to the head of IT in the university in order to implement some changes to the exiting policy about phishing in Canterbury Christ Church University. There will be recommendations made to provide training to students about different types of phishing communication. By the end of the research the goal is to improve the knowledge and understanding of phishing variants from students by implementing changes to the current phishing policy at the university and provide training for students about phishing emails and their variants. A lack of awareness of phishing variants could be problematic because it may lead to malicious cyberattacks by cybercriminals.

Background Research

What is cybercrime?

Europol defines cybercrime as a technical process carried out for a multitude of reasons. The technical process of cybercrime is the sophisticated illegal cyber activities from hackers. Another technical process that is not associated with cybercrime. For example, an employee leaking information about an organisation by publishing personal details of their employees online. Motivations for cybercrime from cybercriminals could be financial gain, stealing personal information, damage critical infrastructure and many other reasons. The nature of cybercrime has led to cybercriminals getting more aggressive with their cyber-attacks. Europol and its partner organisations are one of the lead cyber-defence cross-European governmental law enforcement organisation who are protecting victims from cybercrime within the cyber-warfare arena against different cyber-criminals. Europol published the EMPACT (2018-2021) (European Multidisciplinary Platform Against Criminal Threats) priority. The purpose of this policy is to fight cybercrime by 1) disrupting criminal activities from criminals using different information systems, more specifically those following a 'Crime-as-a-Service' business model and working alongside enablers for online crime. 2) Combating child sexual exploitation and child sexual abuse, which includes the production and distribution of child abuse material, and by 3) taking down and targeting criminals who are involved in fraud and counterfeiting of non-cash means of payment; this includes mass-production of payment card fraud (which includes card-not-present fraud), emerging new threats to other non-cash means of payment and enabling other criminal activities such as different phishing attacks and their variants which is the focus of this thesis (Europol, 2020).

Cybercrime markets sell different illegal products such as hacking tools, services (hacking-as-a-service and fake-identity creations). Examples of cybercrime markets include initial access tools to a system by carrying out arbitrary operations on a machine to deliver payloads. Exploit kits such as Zero-Day vulnerabilities and payloads (malware) on the illegal markets can cause malicious behaviour. Malicious behaviour from malware examples is the destruction of data and data exfiltration. As-a-service offers on cybercrime markets such as botnets or ransomware attack tools (Ablon, 2018). Cybercrime is a process by which criminals target computers or use computers as tools to carry out illegal activities (Islam and Ozkaya 2019).

There are different types of cybercrime: email and internet fraud, ransomware attacks, and theft of financial or card payment data. The study will focus on phishing emails and their variants as a form of cybercrime. A phishing campaign is different types of communication sent to victims to give private information. Phishing campaign messages may contain malicious links or attachments, or they may ask people to respond with personal information. Another form of phishing campaign is spear-phishing. These are targeted attacks that try to defraud specific victims (Kaspersky, 2021).

Cybercrime is a criminal activity that involves a computer, networked device or a network (Brush, 2020). Cybercrime is divided into two categories which are cyber-dependent crimes and cyber-enabled crimes. Cyber-criminals who carry out cyber-dependent crimes use a computer network or computer networks. For example, cyber-dependent crime is when an individual or a group of people gain unauthorised access into a victim's network, this term is also called hacking. Cyber-enabled crimes (online fraud, purchasing of illicit items such as drugs, abuse videos on the surface web or on the Dark Web marketplaces or. onion sites) which all may be conducted online or offline, it can be conducted quickly and distributed at a large scale (National Crime Agency, 2020).

Most cybercrime incidents fall into two main categories: 1) criminal activity that targets and 2) illegal activity that uses computers to commit other crimes. Online criminal activities target computers with viruses and malware variants. Cybercriminals may infect computers with malware and viruses to damage devices or stop them from working. Some may use malware to delete or steal data. Cybercrime that uses computers to commit other crimes may involve using computers or networks to distribute malware, illegal information or illegal images. Some cybercriminals conduct both categories of cybercrime at once. They may target computers with viruses first. Then they use malware on other machines or throughout a network (Kaspersky, 2021).

Online fraud, also known as cybercrime, covers crime that takes place online. Online fraud committed using computers or assisted by online technology (Metropolitan Police, 2021). Phishing is cybercrime is a focus of this study. Phishing variants target or targets people by email, text message or telephone. Different phishing communication appear from a legitimate source to lure people into providing sensitive information (Phishing.org, 2017). Phishing attacks in cybercrime send fraudulent communications that appear to come from a legitimate source. The goal is to steal sensitive data or install malware on the victim's machine (Cisco, 2021). Cybercrime can lead to long-term effects for victims who are

individuals or companies. One of the negative impacts of cybercrime is financial losses for victims and companies.

The cost of cybercrime

Cybercrime is a national scale issue. The cost to the economy is estimated to be £27 billion (Office of Cyber Security and Information Assurance in the Cabinet Office, 2020). According to the Office of National Statistics (2020) in England and Wales the financial loss from fraud varies and can be up to £40,000 or more. Crimes such as fraud are passed to the police for investigation by the NFIB as a case for investigation, the Force Area (with exception of fraud relating to the railways). The order of priorities is 1st A police force area responsible for the fraud investigation covering the location of the fraudulent operation/suspect's address or for business related fraud the office address/place of work of the criminal. (The term for 'business related' fraud means it applies to corporate employee fraud, abuse of position of trust from an employer, boiler room addresses etc). 2nd The police force area with the highest volume of individual usage of credit industry/banking or offences in a specific a geographic area. 3rd The police force area where a victim resides or works. 5th in some rare incidences that it is not possible for a Force Area to use these principles the NFIB will determine a force area (Home Office, 2020).

Europol (2019) stated that phishing has been around for a long time. Phishing may be used as a facilitator from some criminals by using a range of tactics to gather private information from victims. The proliferation of leaked email addresses and the increased numbers of phishing attempts are growing. It can lead to a surge of unique phishing sites detected being at an all-time high. APWG identified 225,304 phishing sites in October 2020 (APWG, 2021). The cost of online fraud of online scams from UK citizens who have shopped online and who may have experienced fraud was estimated to be £1.4 billion (Office of Cyber Security and Information Assurance in the Cabinet Office, 2020).

Approximately \$17,700 (£12,708) is lost every minute because of phishing attacks globally (RiskIQ, 2019). According to Rosenthai (2020), 75% of international organisations experienced a phishing attack in 2020. Verizon's 2020 Data Breach Investigations Report (DBIR) found that 22% of data breaches in 2019 involved phishing because phishing attacks are the top threat action variety in data breaches (Verizon, 2020). The cost of a Data Breach Report from IBM and the Ponemon Institute researchers found the average

financial loss from a data breach from phishing attacks was from human error \$3.5 million (£2.5 million) (IBM, 2019).

Kaspersky Lab (2021) detected phishing attacks against targeted organisations such as banks, payment systems, global internet portals and online shopping in 2020. 18.12% phishing attacks globally targeted online shopping due to the growth in online orders because of pandemic-related restrictions (Kaspersky, 2021). Kaspersky antivirus blocked and detected 184,435,643 malicious phishing email attachments around the world in 2020. The anti-phishing tool by Kaspersky was able to block 434,898,635 attempts at redirecting users to phishing web pages (Kaspersky, 2021).

Smishing fraud or fraudulent Short Messaging Services (SMS) cases are increasing, and it has been reported that it has caused millions in losses among users. For example, losses due to authorised push payment (APP) fraud were £455.8 million in 2019. APP fraud can be from smishing attacks from online platforms used by criminals to defraud victims (UK Finance, 2020). This could be due to the awareness levels of these fraudulent techniques because some people may consider a text message as trustworthy. This type of smishing attack may result in a security attack in which the user may run into a risk of downloading Trojan horse, virus or other malware into their cellular phone or other mobile device. The financial costs of smishing according to the UK trade body UK Finance states that they had lost £1 million a day to bank fraud and more than £207 million in the first six months of 2019 alone. Smishing is a dangerous variant of phishing attacks because people do not expect a simple text message to be malicious. Additionally, the number of SMS open rates are as high as 98% which means that SMS messages are extremely effective in being spread globally to people which may make it lucrative for criminals (Lunn, 2020).

Online fraudsters use fear tactics within their phishing emails to defraud users. Action fraud had several reports from February 2020 about coronavirus-themed phishing emails which include malicious attachments encouraging people to click on a link or download an attachment. Some phishing messages may use emotional and fear appeals goal resembles authentic communications from companies as persuasive elements in different phishing emails (Workman, 2007). The National Fraud Intelligence Bureau had identified 21 reports fraud whereby Coronavirus was mentioned, and victims lost over £800k. The phishing emails about coronavirus encouraged people to provide personal and financial information. The tactic used by cyber-criminals is contacting victims claiming to be from

research organisations associated with the Centres for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) (Action Fraud, 2020).

According to the Crime Survey for England and Wales (CSEW) (2019) fraud victims did not incur any financial loss in around one in four (24%) incidents in the year ending March 2019. This was lower than the previous year and the year ending March 2017 (both 30%). The majority 58% incurred a loss of less than £250, with the median loss being £167. The remainder 15% incurred a loss of £1,000 or more, with 2% of people in England and Wales losing £10,000 or more (Office for National Statistics, 2020). The threat from fraud-based crime on data collected in 2016-2017 from the Crime Survey of England and Wales revealed there was 3.4 million incidents of fraud

The police data of up to 400,000 fraud reports may not been processed and referred to the police due to a 15-month long IT issue, a Which? Money Investigation revealed. Failure of processing of the data sharing between the National Fraud Database which is maintained by Cifas- describes itself as 'the UK's leading fraud prevention service- and the CLP's NFIB. The crime reports were not automatically shared between Cifas and CLP from October 2018, when CLP launched a new crime-reporting service, until recently. According to Which? Money Investigation (2020) stated: '...we estimate that at least 300,000 fraud cases weren't referred to police since the problem began, but that number could easily be as high as 400,000. The year before the data feed went down there were high numbers of crime reports made to NFIB made through Cifas then there were from members of the public through Action Fraud (Which? 2020).

Fraud cases which are recorded does not explicitly state the statistics collected by police forces around England and Wales. The vast majority of fraud reported to the police via Action Fraud is not allocated to a police force. Thus, investigation remains with NFIB with the purpose of intelligence (todayadvisory, 2020). Police Foundation and Perpetuity Research (2018) found that fraud cases are 31% of all crime. More than one-third of victims' report that the impact of fraud was severe or significant for them. But this was not prioritised by the police (The Police Foundation, 2018).

The Police Foundation and Perpetuity's analysis of crime data and interviews with national and local practitioners found that the system which handles fraud reports is poorly structured. Fraud prevention messages are confusing. Also, the victim support services do not meet the specific needs of fraud victims. The research found that the police received 277,561 reports of fraud in 2017-18. Only 8,313 (3%) led to criminals prosecuted. Opportunities to investigate fraud cases can be lost. It happens when victims do not get updated about their fraud cases by the police. Victims' fraud cases often are distributed across the fragmented network of local and national fraud prevention agencies. Some police forces offer limited support or no support to their local fraud victims (The Police Foundation, 2018).

The research found different factors for police not investigating fraud cases. There are 0.8% of the police workforce who work in specialist economic crime teams means there is a lack of dedicated resource for dealing with fraud. 78% of the police workforce said they need more training to deal with fraud. 74% of police employees said they do not have time to deal with fraud cases. Police Foundation's director Dr Rick Muir stated there is no national strategy to deal with fraud cases despite being a third of all crime. The majority of police forces do not have cross-border crime such as fraud to investigate (The Police Foundation, 2018).

Moreover, according to the chair of the Police Foundation's strategic review of policing (Sir Michael Barber) stated that the public needs to change their thoughts and 'think radically' about the role of police forces in England and Wales. He stated the importance of police service future needs to look at various angles because the future of policing will change radically in a few years' time. The current approach to policing might be suitable for the time being but today more and more people are affected by the negative impact of cybercrime. One of the key challenges is keeping the public safe from threat actors who operate globally for malicious purposes. He said that police forces need to think afresh about their future and evolve the police workforce and how the police service is operated and organised (Dearden, 2020). The focus of the study is phishing and its variants. The definition of phishing is a broad term used to describe different types of social engineering attacks against victims.

What is Phishing?

Phishing is a method of conducting cybercrime through the use of social engineering. Phishing variants attacks are carried out by cybercriminals, organised criminal groups, nation-states, hacktivists, malicious actors, fraudsters, and script-kiddies. Phishing can be used in the context of espionage, fraud, and extortion or to launch other cyberattacks against private or public organisations or against a group of people/an individual victim. It is an attack that varies in sophistication that makes the detection of some phishing variants challenging. According to NCSC (2020) social engineering is when a fraudster or group of hackers carry out specific actions in order to gain personal information, that is of some use for the fraudsters. Social engineering attacks has become advanced and the susceptibility of users becoming victims of phishing variants has increased which may have led to one of NCA operational priorities to evolve their intelligence of existing and emerging serious and organised crime threats to the UK which includes social engineering attacks.

Social engineering attacks use psychological manipulation to defraud people and trick them into performing actions or revealing personal information about themselves or other people. Different threat vectors that coexist with phishing attacks stem from different origins and techniques of choice from cybercriminals. Some phishing attacks features may target victims by mistakes they make. Interpol defines social engineering as a broad term used to describe scams used by criminals so that they can exploit a person's trust for financial gain or to obtain classified or private information from a user to enable a subsequent crime. Criminals can use social media as a preferred channel, but it is not strange for cybercriminals to make contact by telephone or in-person with a criminal or criminals (Interpol, 2020).

Phishing threat vectors exist from unexpected scenarios like the coronavirus pandemic. This particular scenario is ideal for cybercriminals who launch phishing attacks that aim is to destabilise victims emotionally. Baiting attacks such as pretexting within phishing communication may lead to some people defrauded from COVID-19 themed phishing attacks (Logsign, 2020). Baiting in phishing is when the victim emotions: temptation, fear and greed as a lure to encourage them to disclose personal details (Keepnet Labs, 2020).

Pretexting is a form of a phishing attack in which a person creates a phishing themed scenario to convince victims to provide personal information (Mason et al. 2014). Other forms of phishing attack vectors are categorised as a social engineering attack which are used to steal data like credit card numbers and login credentials. Cybercriminals goals are to compromise systems to gain private information such as passwords, account information and financial data. Phishing attack vectors take many forms such as: email phishing, cloud storage phishing and mobile phishing (Align, 2018).

Furthermore, other targeted phishing has occurred before the COVID-19 pandemic. For example, in September 2013, a Cryptolocker ransomware infected 250,000 computers from a compromised website or sent to victims from two types of phishing emails. The first phishing email was about a customer complaint and targeted businesses with a Zip archive attachment. The second phishing email had a malicious link about a problem clearing a check and targeted the general public. Once clicked, Cryptolocker encrypted files on the computer and demands the owner make a payment in exchange for the key to unlock and decrypt the files. Other examples of targeted phishing attacks were phishing kits sold on the Dark Web to cybercriminals. The phishing kits allowed anyone who downloaded it to create phishing emails and redirect sites that replicate well-known companies that collects personal and financial information from victims (Phishing.org, 2021).

Phishing attacks can bypass anti-phishing software, firewalls, and domains that blacklist certain phishing websites. Phishing attacks use technical and social vulnerabilities to defraud users. The majority of cyberattacks begin with phishing variants that may encourage victims into malicious websites where malware might be hidden (Hong et al., 2020). Police forces responded to the surge of fraud and cybercrime cases has increased. For example, malware drive-by downloads redirect victims to malicious phishing websites can be harmful. Victims' computers are infected when attachments in a phishing email use a malware drive-by download attack. The attachments could be for a job seeker's CV which might be sent to a HR staff member. These attachments could have malicious embedded code. The most common type of malicious code used by hackers is ransomware. In 2017 it was found that 93% of phishing emails had ransomware attachments (Fruhlinger, 2020). There are different types of phishing variants used by fraudsters.

Phishing Variants

Interpol defines 'Phishing, Vishing and SMShing/Smishing' as: *'Fake emails/text messages/telephone calls purporting to be from a legitimate source such as a bank or e-commerce site are used to induce individuals to reveal personal or financial information'* (Interpol, 2020). Online fraud is a unique type of cybercrime because there is communication taking place between the victim and offender. Additionally, the majority of victims willingly send their personal details, money or other valuable items to criminals. Thus, most fraud victims should not be seen as to be passive actors in their situation; instead, they are an active contributor to the offence, and it is this relationship and interaction between the victim and the fraudster that leads to victim blaming of fraud victims (Fox and Cook 2011). It can be difficult to disentangle online fraud as a large proportion of victims do not know how their identifying information was stolen and this could be via cyber-identity theft, smishing, phishing emails and fraudulent calls (Roberts, 2008).

Different types Phishing emails, Vishing and Smishing will be the focus of the study which are fraudulent emails/text messages/telephone calls which all claim to be from a legitimate source such as a bank or e-commerce site are used to defraud people to reveal personal or financial information (Interpol, 2020). Interpol (2020) stated that COVID-19 fraud scams that are associated directly with the virus are: phishing emails and telephone fraud. For example, phishing emails are used in the COVID-19 pandemic to defraud individuals such as: '2020 Coronavirus Updates' and 'Coronavirus Updates'. The phishing emails target people who may be curious to know more information about the pandemic. The content of the covid-19 themed phishing emails contained attachments that distributed malware and ransomware or lead users to fraudulent websites to collect user credentials. The content of the emails were worded in a manner that they persuaded users to visit websites that cybercriminals used to collect personal information from victims (Cybersecurity and Infrastructure Security Agency, 2020).

Believable phishing emails and their variants are fraudulent communication that trick people into believing that they are from a trusted source (Hahnagy et al. 2015). Phishing variants persuasive techniques used by fraudsters in different types of phishing communication (Tandale and Pawar 2020). The sophisticated nature of the phishing variants sent to victims can increase the chance of being defrauded (Ivanov et al. 2021). Victims of online fraud may provide their personal and financial information to cybercriminals and fraudsters. Fraudsters want to make money illegitimately by sending phishing communication to their victims. Cybercriminals use a variety of techniques to initiate phishing attacks-some of the phishing variants are email, social network, VoIP (voice phishing), SMS (smishing), malicious websites, search engines, and instant messaging (Smadi, Aslam, and Zhang, 2018).

Cybercriminals use various online fraud techniques in order to steal personal information and money from victims. Phishing emails, identity theft and fraudulent calls (vishing calls) are used when cybercriminals pretend to be someone else. Additionally, online scams and phishing is carried out by threat actors who often create COVID-19 themed phishing emails impersonating government and health authorities. Cybercriminals use different tactics to defraud victims into providing their personal information and may download malicious content on their computers. According to Interpol (2020): *'Around two-thirds of member countries which responded to the global cybercrime survey reported a significant use of COVID-19 themes for phishing and online fraud since the outbreak'* (Interpol, 2020).

The sophistication of smishing (Short Message Service Phishing) is a text message sent by a fraudster or cybercriminals to persuade victims to reply to the text message or call the premium number in a text message. Smishing is another variation of phishing that involves a text message which is a text message sent on to victims' phones to encourage people to call a specific phone number or log on to a Web site from a link in a smishing text message (Reynolds, 2011). Smishing's purpose is to steal a user's credentials over a mobile phone by clicking on a link that directs them to a fake website or redirects them to a fraudulent app user interfaces (UI) through which the user gets tricked into disclosing sensitive information (Felt and Wagner, 2011). Cybercriminals prefer to send out smishing texts. Mobile phone applications ask for user credentials when a specific mobile app is open can increase the likelihood of a smishing attack to be successful (Marforio, et al., 2016).

One of the most dangerous types of phishing attacks is spear phishing emails. Spear phishing emails appear to be from a trustworthy source (Shakela and Jazri 2019). Cybercriminals who send spear-phishing emails research the victim. The information about the victim can be collected from different sources such as social media information or public posts on social media, third-party websites and breached third-party websites may have some personal information about the victim (Sameen et al., 2020). Sensitive information shared on social networking sites can be viewed by hackers. Information about employees found on company websites can allow hackers to find names of a victim's friends, colleagues from their Facebook account, LinkedIn profile and find out about their hobbies and current company projects from their Twitter feed (Giandomenico, 2020). Once specific information collected from the victim is used to send a spear-phishing email (Xiujuan et al., 2019). Spear-phishing emails are unique to a specific recipient and refer to existing information found on the internet about a victim. Spear-phishing emails can make the email looks official when received by the recipient (Allodi et al., 2020). Spear phishing emails are more likely to be opened when they appear to be from a trustworthy source (Caldwell, 2013). Also, this will be looked at further within this study if some students fall victim to some spear-phishing emails. Students' lack of awareness from spear-phishing emails may be evident from the anonymised questionnaires and a focus group.

Modification of the phishing URL of a single character can make detection difficult. Thus, the blacklist of phishing domains might store old phishing URLs. There is also an issue of targeted phishing attacks such as zero-day spear-phishing emails that may not be on blacklists sites. (Vayansky and Kumar, 2018). Furthermore, new phishing sites are known as zero-day (0-day) phishing because they will not be identified as phishing until it is on a blacklist phishing domain. The study found that this is a vulnerability to the blacklist phishing domain and can result in a phishing attack which could often take hours or months registered into blacklist domains. It can increase the likelihood of zero-day phishing attacks sent to multiple users (Aieroud and Zhou, 2017; Srinivasa et al., 2019).

Email phishing variants are a numbers game. A group of hackers or individuals who send fraudulent messages can gain a substantial amount of money, even if only a small percentage of victims respond to phishing variants. Some hackers create phishing messages that appears to have come from a legitimate business. They may use the same phrasing, typefaces, logos, and signatures and can make the phishing email appear from

a specific organisation. It does not take a long time for hackers to create phishing communication because phishing kits can be used (Doupé, 2018).

One of the issues with phishing attacks is it may grant criminals access to governmental or organisations networks which are part of a larger attack, such as an Advanced Persistent Threat (APT) event. APT uses sophisticated hacking techniques to access a system. An APT threat is stealthy threat actors who may be nation-state or state-sponsored groups. APT hack computer networks and remain undetected for a specific period of time. Threat actors' motivations could be economic or political (Kaspersky, 2021). In this specific example, employees' personal information is compromised in an APT event by hackers who can bypass security perimeters, spread malware within the system, or gain access to secured data (Imperva, 2020). Furthermore, some people may find it challenging to identify phishing email variants because cyber criminals might make the phishing email appear official. They might be more likely to be victims of phishing email fraud. Also, some phishing emails can bypass and fail to be detected using conventional, signature-based and sender verification techniques due to new phishing style attacks that involve advanced social engineering techniques. Some phishing attacks do not focus only on stealing personal information and spreading viruses but extending to high impact data breaches and ransomware (Ayob and Weir, 2021).

There are different strategies used by fraudsters to victimise individuals from phishing emails: syntactic (technical), semantic (social engineering) and blended (both) (Smith 2010). Fraudsters use syntactic strategies by exploiting vulnerabilities to access personal data through malware such as spyware: software that allows a user to gain covert information about another person's computer activities by transmitting data covertly from their hard drive. Viruses is a piece of malicious code that can copy itself and typically has a detrimental effect, such as corrupting a system or destroying data. Trojan-horses: might typically pose themselves as or embedded in a legitimate programme, but it is designed for malicious purposes, such as theft of data, deleting files, expanding an existing malicious botnet, spying, and carrying out DDoS attacks. Worms: in a phishing email to replicate itself over a computer network and performs malicious actions without guidance (F-Secure, 2021). Keyloggers: can be used in some phishing emails within attachments. Malicious spyware within the keylogger software can capture private information like passwords and, financial information can be sold on underground forums to third parties for criminal activities (Umarani and Sengupta, 2020). Fraudsters use semantic techniques

as a form of social engineering. Victims can send their personal information by being tricked by semantic strategies from different types of phishing emails, smishing (texts messages), social phishing (social network sites) and vishing (phone-calls).

Cybercriminals use fraudulent emails or websites using official company trademarks and logos to represent financial institutions or an Internet Service Provider (ISP). Online shopping and bank themed phishing emails can be targeted by pharming attacks. An advanced form of phishing is pharming which redirects the connection between an IP address. Cybercriminals carry out pharming by breaching the Domain Name System (DNS) server through social engineering.

Pharming targets a user who wants to browse to a website and its target server is a specific website. A user is redirected to a fake website when a user clicks on a fraudulent link. The user unknowingly gets diverted to a mirror website (Ivanov et al., 2021). Cache poisoning is used against the victim to enter their personal information can compromise their computer system. Pharming can also target a local machine that uses a trojan to modify the host file (Britz, 2013). DNS cache poisoning or DNS spoofing is an attack that exploits vulnerabilities in the DNS to redirect internet traffic away from servers belonging to a specific website and towards fake servers. Once the victim visits a fraudulent website hosted on a fraudulent server and enters their personal information, cybercriminals can sell their personal information on the Black-Market, darkweb or illegal underground websites. Some people may not be aware of the hacking methods used in this type of phishing fraud (Aijaz, Misbahuddin, and Raziuddin 2021).

High technology fraud offenders are not the average person who is stereotyped in the media (Fox and Cook 2011). The majority of cyber criminals commit fraud for the same reasons that most criminals commit crimes: motive, opportunity, and rationalisation (Holt et al., 2015). High technology fraud offenders differ little from the average criminal in terms of their motivations in their methods to commit crime are different. Cybercriminals use electronic device/devices; some cybercriminals use both technology and criminal activity offline. Studies also indicate that most computer crimes are for personal financial gain, followed by cybercriminals needing to be intellectually challenged, to help organised crime groups and as a result of peer pressure or to gain peer recognition (Holt, Bossler, and Seigfried-Spellar, 2015).

Malicious techniques used by botnets are often upgraded and become complicated for digital forensic investigation. The majority of botnet writers may use enhanced network technologies and a standardised software environment. Cybercriminals may use advanced anti-forensic techniques which may make it challenging for a digital forensic investigator to conduct analysis on botnets. Cybercriminals use botnets for running arbitrary network services for phishing. In a phishing attack, a botnet has been used as servers for sending phishing emails and host phishing pages. Thus, forensic investigation of botnet cybercrime is fundamental to analyse bot malware and understand its functionality (Sarkar, 2018).

Police forces may not have the capabilities or resources to prosecute criminals for fraud. Cybercriminals use TOR encryption software. TOR is used for anonymisation when conducting illicit activities such as sending different phishing attacks to recipient's email addresses. Police forces in the UK should work collaboratively with international law enforcement partners in investigations involving the sale of fraudulent information. Digital forensic specialists in international police departments should investigate the sale of fraudulent data on the Darkweb and anonymisation software used by cybercriminals to hide their illicit activities (Europol, 2014). Furthermore, VPN is fundamental because over 12 billion user records, including names, addresses and credit card details are stolen every year. By 2023, it will be 33 billion records a year (Kaspersky, 2020). There are different phishing countermeasures to combat malicious phishing communications.

Anderson (2008) demonstrated how banks are dedicated in combating fraudulent banking emails by attempting to raise awareness by looking for indicators of a phishing email, but fraudsters are including features within an email which are advised by banks to make the email appear trustworthy. Banks made different recommendations to customers: 'Check the English' fraudsters amended their phishing emails by either using the banks' own emails but with fake URLs or got an individual who could write English. Banks then advised customers to 'Look for the lock symbol' so when the user got redirected from the hyperlink from the phishing email to the phishing sites it had started to use SSL (or just forging the graphics of lock symbols on their web pages). The banks advised customers not to click on images and URLs; the fraudsters then devised a method to put in links that appeared to be images but were executables (Goutal, 2019). The next advice was then to check where a link would direct the user to by hovering their mouse over it; the fraudsters used a non-printing character into the URL to stop Internet Explorer from displaying the rest or

used long URL (as the majority of banks also did). Fraudsters who deploy new tactics within phishing emails to defraud victims signify that individuals can still be defrauded even if they are aware of the recommendations made from banks about phishing emails.

Most anti-phishing techniques use source code-based features and third-party services to identify phishing websites. These techniques can have limitations. They are vulnerable to drive-by downloads from phishing variants. Anti-phishing tools that use third-party services to detect phishing URLs can delay the classification process (Rao et al., 2020). Moreover, phishing websites designed to be replicas of trusted websites. Anti-phishing tools in usability studies showed that the server-side security indicators and client-side toolbars and warnings be ineffective in preventing vulnerable users from being defrauded. Fraudsters can use pharming which uses internet vulnerabilities based on a DNS server and DNS resolver. Phishing attacks use pharming use malicious links to redirect users to phishing websites. Pharming phishing websites replicate websites (Sheikh, 2020). Some users could not know how to interpret security cues. Other users ignore anti-phishing toolbar warnings (Yue and Wang, 2008).

Security tools may not eliminate all security threats and vulnerabilities from phishing variants, but they can detect security vulnerabilities in a system (Sudhakar and Kumar, 2020). For example, fileless malware used by malware authors in spear-phishing campaigns do not download malicious files or write any content to the disk to compromise the systems. The attacker exploits a vulnerable application to inject malicious code into the main memory. In fileless malware the attacker use malware to control the compromised systems locally or remotely (Sudhakar and Kumar, 2020). The security tools can be beneficial to improve security to a certain extent. Programmers could devote more time to patching vulnerabilities regularly. If programmers fix software vulnerabilities, they can detect phishing attacks. However, it does not always happen leaves users exposed to sophisticated phishing attacks. Zhang et al. (2007) found some anti-phishing tools are vulnerable to simple exploits. Other issues with students not using security tools are students are prone to security threats from social and psychological aspects of advanced persistent threats (APT) from phishing variants. Students who are unaware of security toolbars cannot protect themselves against advanced malware attacks within phishing emails.

Some limitations of security toolbars and other browser security indicators are ineffective at preventing some types of phishing attacks. Wu et al. (2016) study that many participants did not notice the security toolbars. Other participants ignored the security warnings if the content is related to malicious phishing websites. Users may not check the browser's security indicators regularly. Managing security might not be the users' primary goal. Some users identified suspicious signs from the security toolbars, but they did not know how to interpret them or dismissed them. There are usability issues with anti-phishing toolbars. Anti-phishing tools can be used to identify the majority of fraudulent websites with fewer false positives but may have usability issues. The users could be vulnerable to phishing attacks (Li and Helenius 2007).

Phishing Countermeasures

PurplePhish provides automated phishing simulations and user awareness training to increase awareness about different types of phishing emails. PurplePhish can help students and employees to identify phishing attacks and security teams to monitor risk and compliance. PurplePhish can provide phishing simulation, spear phishing simulation and cybersecurity training. The training features can be part of staff training for employees and university students. IT support employees can assess employee and students' susceptibility against phishing variants from advanced tracking and reporting within PurplePhish (Digital Marketplace, 2020).

Police use internet evidence to document and collect digital evidence on Internet Service Providers (ISPs) owning an Internet Protocol address (IP address). Digital evidence collected by the police used to prosecute cybercriminals. Information can be obtained on the receiver's PayPal account and associated IP addresses and identify IP ownership from digital forensics employees in police forces (Shipley and Bowker, 2014). Security functions used by digital forensics investigator's purpose is to protect, detect, respond and investigate digital crime such as different phishing attacks (National Institute of Standards and Technology, Gaithersburg 2018).

A forensic investigation method to identify fraudulent transactions from cybercriminals is Artificial Immune Systems (AIS) (De Sá, Pereira, and Pappa 2018). AIS inspired by the human biological immune system. The AIS is a self-adapted system used for credit card fraud detection. The case-based learning model and the genetic algorithm used in AIS can perform online learning instantaneously and enables the capability of fraud detection on online transactions. A separate study by Cavalca and Goldoni's study (2010); (Sarkar, 2018) demonstrated a honeypot used to collect botnet malware variants using external analysis providers. The malware collected and stored in the honeypot system. Then the stored malware are analysed by deploying external services. The investigators can create a database of the collected malware by the honeypot system and gather the information used for malware analysis that may be used for forensic analysis to reconstruct the digital crime incident (Sarkar, 2018).

The NCSC advised organisations including educational establishments should apply a multi-layered set of mitigations against phishing communication. The defence against phishing attacks can be difficult against zero-day phishing attacks. Zero-Day phishing attacks are undiscovered for example until a honeypot is launched against a specific botnet. A honeypot is a term used when a computer system is intended to attract cyberattacks (like a decoy). It stimulates a target for hackers to exploit and use their intrusion attempts to gain intelligence from them and cyber-forensic experts could possibly find the source of the attacks launched by them (Kaspersky, 2020). Moreover, zero-day malware from phishing communication means there is no identifiable signature which can be detected by signature-based security platforms (Barker, 2020).

Wright et al., (2010) research identified Test Grazioli's Theory of Deception within phishing emails includes the user's trust and web experience as two fundamental factors of susceptibility and deception detection in phishing emails and their variants. These are factors to be considered when asking focus group questions that can gauge their awareness levels of different types of phishing communication methods used by fraudsters.

Similarly, four main reasons drive organisations or even educational establishments to implement a security awareness training programme. One of the reasons is compliance which means that regulations are effective. A reason for this could be information dissemination carried out to enable a larger portion of people to be aware of policies, news, concerns, exceptions and manage the security-related actions of employees or students at universities. Behaviour formulation is another factor to consider by influencing and managing security-related incidents of employees and students. Cultural shaping can create the organisations' collective values, beliefs, actions and attitudes. They all relate to cybersecurity when several students could receive phishing variants from various methods used by fraudsters protected by cybersecurity employees and phishing awareness training implemented. (Carpenter, 2019). Moreover, user education is fundamental to raise user awareness of phishing attacks (FSB, 2020).

Cascavilla et al. (2021) recommended packet sniffing to analyse data transferred between infected hosts and observe intrusion activities using botnets using a machine learning approach to monitor forums through Natural Language Processing (NLP) ML and leveraging Open-Source Intelligence. The use of this technique considers phishing, social attack, worms and DDoS. The study conducted an online investigation to determine if the malware steals personal information. Cascavilla et al. (2021) research used a botnet as part of digital forensic analysis. It could provide investigators with an understanding of the intentions of online crime and online criminal behaviour. The botnet investigation systematically analysed data using a complex machine and deep learning investigations. Topic Modelling Analysis analysed and identified threats in the Surface and Deep, Dark-Web (Cascavilla et al. 2021).

There is a low number of sophisticated solutions for mobile phishing, and this could be due to a certain quantity of resources required to deal with the issue in mobile devices. Numerous apps can help prevent smishing text messages Wu et al.,(2015) highlighted the effectiveness of anti-phish mobile tools for Android mobile devices called MobiFish. Joo et al. (2017) found a smishing detection method called S-Detector gathers the logs and timestamp of a smishing attack. The number or URL from the smishing text message gets sent to a blacklist database to see if it exists. The algorithm uses an Android Package Kit or (APK) file downloaded as a package file format. A package file format the installation and distribution of mobile apps for mobile phones with an Android operating system. A Naïve Bayes algorithm used to detect SMS spam once a file has been decoded and gets directed to an unusual path with a risk weight value; it will flag the text message as a

smishing text attack (Baadel, Thabtah and Majeed, 2018). To measure the awareness levels of mobile anti-phish tools for Android mobile phones' people are compared in terms of their technical knowledge on how these applications work to prevent smishing attacks.

A recent study by Sonowal and Kuppusamy (2018) revealed that current methods to detect smishing attacks are possible. S-Detector or Smishing detector differentiates between text messages from smishing text messages. The software used a morphological analyser to extract the noun words used regularly in smishing text messages. A Naïve Bayesian classifier can filter text messages. The experiment result was beneficial because the model enabled security, real-time access and reliability in stopping most malicious smishing text messages and more sophisticated security threats (Sonowal and Kuppusamy, 2018).

Internet users are encouraged to look for security measures on websites when they input financial or other personal information. The letters at the beginning go to the address bar or URL at the top of the screen should change from http:// to https:// this means that personal information entered and transmitted on the website is encrypted. The internet browser may also show that information is encrypted so no-one can intercept data. If data is encrypted, there is no guarantee that the company will store the data securely. It can be seen as a breach of the General Data Protection Regulation (GDPR) if personal information is illegally accessed, stolen or lost from the company (Information Commissioner's Office, 2019).

According to the Financial Ombudsman Service (FOS) (2015), banks are not responsible for 'Vishing Fraud' or Voice Phishing'. Online fraud may have a knock-on effect on the reputations of all businesses involved. For example, prize competitions that need peoples' mobile numbers and non-secure online marketplaces. A data leak can lead to some form of a phishing attack (Glabbeek, 2019). On the other hand, UK Finance stated: 'The banking industry is working with mobile network operators, the Government, and different industry stakeholders to tackle smishing fraud' (Lunn, 2020). A proposed solution to smishing fraud is awareness campaigns within the workplace, schools, colleges, and universities. Awareness campaigns are one way to increase knowledge and awareness among SMS users. However, it is not enough to deal with new types of smishing fraud communication (Tajuddin, Dangi and Marzuki 2016).

There are some countermeasures put in place to prevent people from becoming victims of phishing emails. Email filtering and email authentication would prevent the user from being sent a phishing attack. Email authentication is the process that identifies the origin or domain so that ISPs can find a route for an email. It is a technique used to prevent spoofing and phishing attacks (Kinsta, 2021). Security tools used by some internet users could be phishing toolbars and indicators so that the user can identify a fraudulent website (Davinson, 2010). For example, a DKIM (Domainkey Identified Mail) is a domain name identifier to a message. DKIM uses cryptographic techniques to validate authorisation for its presence (Kinsta, 2021). Email filtering is software that analyses incoming emails automatically and decides if they are phishing emails or not (Kastner, 2020). It can highlight a high awareness level from some users who use security tools to protect themselves from phishing attacks.

CrawPhish is a tool used to harvest the source code of current and previously reported phishing websites. CrawPhish can automatically detect and categorise the client-side cloaking techniques used by phishing websites (Zhang et al. 2021). Fraudsters use cloaking techniques to bypass detection from anti-phishing systems. The phishing websites with cloaking display benign-looking content instead of the phishing page (Oest et al., 2018). Therefore, CrawPhish uses static and dynamic code analysis to find the client-side cloaking techniques used by phishing websites (Zhang et al. 2021). Another phishing countermeasure is FldrNmLnth. The length of a folder name of the URL's path uses FldrNmLnth. FldrNmLnth is a phishing detection feature. The length of folders' names of legitimate URLs on the other side did not exceed 30 characters. This difference in length used as a folder name length is used to detect phishing URLs (Daeef and Saudi, 2020).

Other phishing countermeasures proposed to use an email characterisation calculation by using a Bayesian Classifier. A Bayesian Classifier was used to identify phishing URLs location by a Decision Tree C4.5 (Tareek and Sunil, 2015). Pawan et al. (2010) suggested two methods to identify phishing websites. Introduce heuristics to find the number of known phishing websites and new phishing websites. Another is to use matching algorithms to find new phishing websites. For example, DeepPhish is an automated phishing detection tool with Recurrent Neural Network. DeepPhish analyse text and tangential statements that are indicative of phishing attacks. DeepPhish uses linguistics analysis to monitor content in a phishing email (Arivukarasi and Antonidoss, 2020).

A Convolutional Neural Network (CNN) framework with 18 layers uses Alex Net. Alex Net is for the classification of websites using screenshot images and URLs of phishing and legitimate websites. CNN uses deep, feed-forward artificial neural networks. Artificial neural networks mean connections between nodes do not form a cycle and use different multilayer perceptions designed to require minimal pre-processing (Rajaram and Dhasaratham, 2021).

Studies about internet bots used to research phishing are relatively current to academia because web crawlers are for information extraction. A botnet system such as fast flux botnet catcher system (FFBCS) can detect Fast-Flux (FF) domains in an online mode using an adaptive dynamic spiking neural network algorithm. The FFBCS showed a high level of detection accuracy, low false positive and negative rates (Almomani et al. 2021). Botnets' detection are used for analysis such as the Network forensic analysis flow exporter tools like NetworkMiner, CapLoader and Wireshark. The extracted features are used to monitor the botnet malicious activities (Raheja et al. 2021). Other tools such as WC-PAD use web crawlers to crawl each webpage of a website. Most cyber-criminals do not index all the web links in the phished website. The experiment analysis proved that web-crawlers detect most zero-day phishing attacks (Nathezhtha, Sangeetha and Vaidehi, 2019).

Machine learning methods might use convolutional neural networks (CNN) for high accuracy classification to distinguish genuine sites from phishing sites (Yerima and Alzaylaee, 2020). Malicious URL section and improved email filtering can block some phishing emails when users are using their email online. Jain and Gupta's study (2017) suggested visual similarity-based approaches that compare a phishing page with websites using their visual similarity. However, the phishing detection approaches limitation based on hand-engineered image features might not apply to sophisticated phishing attacks (Phoka and Suthaphan, 2019).

Machine Learning (ML) based security framework analyse the patterns in URL strings. ML is used to address the drawbacks associated with list-based and content-based detection approaches. ML-based detection framework extracts discriminating and uncorrelated URL feature values from URL strings. A baseline profile is in the extraction process of the URL is created as a result. The baseline profile will monitor and identify malicious URLs in real-time. An ML-based framework is beneficial because it does not rely on pre-existing blacklist databases to identify malicious URLs. The ML-based framework can detect malicious URLs associated with zero-day phishing attacks (Kumar and Subba, 2021). Phishing detection at a client and server level is from a study by Lakshmi et al. (2021) used a phishing detection approach used a supervised Deep Neural Network with Adam optimizer to detect fraudulent websites from genuine websites. They identified phishing websites using hyperlinks available in the source code of the HTML page.

Phishing detection tools can detect a phishing website from a web browser on the client side or with specific software at the host. Phishing websites identified at the server side is beneficial because they have minimal reliance on novice Internet users. Search engine-based techniques extract features in a phishing detection tool that extracts images, text and URLs from websites. Legitimate websites may have a higher index than phishing websites, which remain active for a short time. Other phishing countermeasures can be phishing blacklist and whitelist-based techniques. The phishing blacklist and whitelist-based techniques blacklist malicious URLs of phishing websites or whitelist URLs of legitimate websites at the client or a remote server (Varshney et al., 2016).

There is server-side and client-side detection for phishing attacks. Anti-phishing software contains computer code to find phishing websites. These block the content with a warning to the user. Anti-virus and Anti-malware are software's that are in the client-side detection category. Armano et al. (2016) found a real-time method of detecting phishing websites by developing an add on or extension for a browser. Server-side detection proposed by Hu et al. (2016) analyse server log information to identify phishing websites. The user when they visit a phishing webpage, the browser contacts the legitimate website for resources. The request is registered in a log from the official website server to identify illegitimate ones. Similarly, Wu et al. (2019) stated a technique that uses fuzzy logic using machine learning to avoid using a Boolean algorithm in the system.

Anti-Smishing software can prevent smishing text messages: S-Detector, SmiDCA and Smishing Classifier which was not discussed in the focus group by the participants. S-Detector uses a combination of content-based technique and URL based technique for detecting and blocking smishing messages. SMS content is analysed by checking the URL in a text message and smishing keywords in the text message. SMS keywords are analysed and classified using Naive Bayesian classifier. The URL in the text message is checked whether it downloads an APK file while invoking the URL. Text messages which contain a higher quantity of smishing keywords or a URL that downloads an APK file are categorised as smishing messages. SmiDCA is a smishing detection model which used: machine learning algorithms, heuristic methods and content- based feature extraction to differentiate smishing messages and text messages from non-malicious sources (Sonowal and Kuppusamy 2018).

User Awareness Studies on Phishing Variants

Jagatic et al. (2007) stated in their study that awareness of phishing email among users has increased, but so has the sophistication of phishing emails has evolved. Thus, there are still victims of this type of fraud. Fraudsters create phishing emails that evoke psychological emotions like greed and fear. The majority of spear-phishing emails target specific groups of people to gain their personal information. Fraudsters make a spear-phishing email look genuine by contextualising the email by incorporating personal information. Users' lack of technical knowledge to identify vulnerabilities and spear-phishing emails is problematic (Hong, 2012; Purkait, 2012). The data collected from the study found that demographics and phishing susceptibility amongst younger participants aged 18 to 25 performed worse than all of the other age groups could be due to fewer years of experience online, lower awareness of risk and less exposure to training materials. For instance, individuals do not know phishing email techniques used by fraudsters (Kritzinger and Von Solms, 2010; Kritzinger and Von Solms, 2013).

Real-world phishing research studies is when researchers create a phishing email and sent it to people who are not aware that they are participating in a study. Real-world phishing research studies can assess people's gap in knowledge and believability of the phishing email they have received. Overall, this shows the creative and sophisticated nature of real-world phishing research. For example, in Jagatic et al. (2007) phishing email study, over 900 university students were unaware that they were part of the study. Researchers used information on Facebook and Twitter to identify the friendship groups of the students. Half of the students received a phishing email that appears to be from one of their friends. This social engineering tactic used in this study is highly effective because of the phishing email's social context. 72% of these students clicked on the link and provided their personal information.

A possible solution to thwart spear-phishing is regular staff training to remind employees that safe email practices are fundamental. Employees in the workplace should be encouraged to report a suspected cyber-attack rather than ignore it. Another recommendation to hinder spear-phishing emails is for employers to share information with employees via email or the local staff intranet about the types of attack that have been received by other people in the organisation so that staff members will be aware of fraudulent emails. Employers could display examples of phishing emails on the local staff intranet or be sent an email about phishing emails and their variants. IT staff members can check phishing emails when reported by employees (Caldwell, 2013).

Nonetheless, as phishing tactics become increasingly sophisticated, spear-phishing emails appear to be authentic. For example, attackers may include subject lines that would be topics of interest to the recipients to trick them into opening the message and clicking on attachments or links (Tehrani and Pontell 2021). Thus, organisations from different sectors need to consider different approaches to tackle the threat, such as training employees on spear-phishing and taking into account the different awareness levels of fraudulent emails .

Pattinson and Jethat et al. study (2011) illustrated that people who are more familiar with computers managed to phish better than those who are not. The findings were predictable because people who had technical knowledge are likely to be aware of risks and consequences associated with phishing emails than people who do not use computers regularly (Pattinson and Jerram et al., 2011). It may affect the data collection sample of this research by indicating the students' lack of awareness of phishing communication

who may have no technical knowledge. Some students who may know about phishing variants may be aware of the risks from phishing emails. Pattinson and Jerram et al. (2011) study show that those who are not told before the survey that this was phishing study their familiarity with computers did not correlate with how they dealt with phishing emails. In terms of managing genuine emails, the familiarity had no significant impact on being a victim of phishing emails and their variants. It is fundamental to consider training programmes, organisational procedures, and security tools to measure awareness levels of different types of phishing emails and their variants (Williams et al. 2017).

High rates of victimisation from phishing emails and their variants are because people fail to identify features in a phishing email (Vishwanath et al. 2011; Workman, 2008). Around half (54%) of fraud incidents in the year ending March 2019 were cyber-related which includes phishing email attacks (Office for National Statistics, 2020). It will be looked at further within this study by analysing, assessing and finding the weakest knowledge of phishing variants are from Canterbury Christ Church students' awareness levels of phishing emails from anonymised questionnaires and a focus group.

A study aim was improving individuals' ability to find cues used in phishing emails from fraudsters (Kumaraguru, Sheng, Acquisti, Cranor and Hong, 2008). In a series of studies entitled the Carronade Experiments conducted at West Point, army cadets trained to recognise phishing emails before sending them real phishing attacks (Ferguson, 2005). The research found that education and training are not enough to spot deceptive cues within phishing emails, and it is only beneficial in the short term. Most of the participants were victims of the phishing attacks within four hours after the educational intervention (Ferguson, 2005). Thus, according to Ferguson (2005), education and training may be ineffective. Individuals overloaded with information about phishing emails struggle to process all of the information provided. It could link in with the disadvantages of student phishing training sessions. Some students may not remember all of the information provided to them about phishing attacks at Canterbury Christ Church University.

Higher education establishments are targets of different phishing emails. Duo Security identified that 72% of UK universities which responded to the Freedom of Information (FoI) request had reported falling for a phishing attack (Kleitman, Law and Kay 2018). On the other hand, fraudulent phishing emails from Furnell's 2013 study with Barclays Bank can be sent to students in universities, whereby they are persuaded to provide their personal

details to cybercriminals. Another factor which could increase the likelihood of students to become a target of a fraud scam is the disclosure of personal information on the internet from online activities. The study carried out by Mesch and Beker (2012) highlights that students who reveal too much personal information from their online activities such as on social media can expose themselves to fraud, identity theft and cyberstalking.

Additionally, Wang et al.'s, (2012) study draws upon the theory of deception of defrauding students from phishing emails. The research model suggests that the overall cognitive effort when processing emails decreases with attention to visual triggers and deception indicators in a phishing email. Visual triggers in phishing emails is making the content of the malicious email look similar to a legitimate email such as using similar domain names and visual design (Dhamija et al. 2006). Deceptive indicators in a phishing email's content creates a sense of urgency so that the user does not notice it is a phishing email (Irwin, 2020). Other deceptive indicators in some phishing emails is email spoofing which is when an attacker send emails with fraudulent sender addresses as part of a phishing attack designed to steal a user's information, infect their computer with malware or request for money (Malwarebytes, 2021).

According to the National Crime Agency's (NCA's) National Strategic Assessment (2018), social engineering is a facilitator of cybercrime because cyber-enabled fraudsters have limited cyber skills or are highly skilled cybercriminals. For example, cyber-enabled fraudsters have a range of skills. They can be a script kiddie to an elite hacker. Criminals predominately use previous weaknesses or zero-day exploitations by using phishing kits in social engineering to exploit victims in cyberspace. It may make spotting potential weaknesses shown in phishing emails and their variants challenging to identify. For example, poor grammar or spelling in emails or other phishing variants that a communication sent by online fraudsters is fraudulent and potentially malicious. Spamming and phishing are a significant threat within the cyberspace landscape is based upon an industry survey of 100 UK IT professionals: 75% had dealt with a security incident about a phishing email (NCA, 2018).

The next section will explore the methodological approach by including overall description of the overall methodologies explored in the study, section of methods used in relation to the research questions, ethics approval process, participant information and data collection such as anonymised questionnaires and focus group process.

Methodology

Qualitative and quantitative data collections methods are in the study. Quantitative research focuses on objective measurements, statistical or numerical analysis of data such as questionnaires. Quantitative research generalises groups of people to explain a particular phenomenon (Babbie, 2010). Qualitative research is a data collection method including observations, textual, interviews (individual or group) and focus groups (Gill et al., 2008). Qualitative research involves non-numerical data such as text, video and audio (Bhandari, 2020). A mixed-method approach in the study will combine quantitative data collection from anonymised questionnaires and qualitative from a focus group. It can be advantageous due to increased verifiability and a social context in answering the research questions. A mixed-method approach is a methodological approach that intersects mixed methods and combining them with other data collection methods. A mixed method as a methodological technique is when a researcher uses: questionnaires and a focus group in their research study (Axinn, Fricke, and Thornton 1991; Edin 1999; Axinn and Pearce, 2006).

Mixed method data collection uses the strengths and counterbalances the weaknesses of other data collection methods. Creswell and Plano Clark (2011) noted that during data collection when the results from the strand (quantitative or qualitative) can establish data collection in the next strand; therefore, the two study strands are connected (Ivankova, 2014). A fundamental principle of research mixed methods is that it is mixed in a way that has complementary strengths and non-overlapping weaknesses. A mixed-method approach recognises that all data collection methods have limitations and strengths (Tashakkori and Teddlie, 1998). The use of quantitative and qualitative data are usually combined. Thus, the findings are merged and interpreted together (Bachman and Schutt, 2013).

A mixed-method approach allows a framework to provide practical explanations. Therefore, some level of analysis can take place. This approach will enable a range of data and methods to be combined and integrated (Bryman, 2008). Anonymised data collected from a focus group and questionnaires will include awareness levels of phishing fraud from students. It can apply when gauging awareness levels of phishing emails from students at Canterbury Christ Church University and their perception of different phishing emails and their variants.

Selection of methods in terms of research questions

Research Question 1: What are the underlying factors in which students fall victim to different types of phishing attacks?

In the study, anonymised questionnaires with (Third year) Policing and (First year) Criminology and a focus group with (First year) computing students to assess the numerous underlying factors that may lead to some students victimised from phishing variants. The aim of a survey or a questionnaire is to obtain information which can be analysed, and patterns extracted, and comparisons made. Questionnaires are used to describe a population or characteristics of that population. Data collection techniques appropriate to survey research are questionnaires, structured interviews, and direct, structured observation (Pickard, 2013). The purpose of the focus group discussion in the study is to gain an in-depth understanding of social issues. The method aims to collect data from computing students rather than from a statistically representative sample of a broader population of students (Nyumba, et al. 2018). Questionnaires were chosen to find the underlying factors in which students fall victim to phishing attack variants. Questions that measure knowledge was used to assess students' familiarity with a subject. The questions are used to gauge students' ability to provide informed responses (Fowler and Floyd 1995).

Research Question 2: Does the perception of different types of phishing emails from students correspond with statistical information in a focus group and anonymised questionnaires?

Perception of students about phishing variants from specific subject areas within the School of Law, Policing and Social Sciences at Canterbury Christ Church University and the School of Engineering, Technology and Design. Questionnaires can elicit information about attitudes that are difficult to measure using observational techniques (McIntyre, 1999) about the students' perception of different types of phishing emails. Also, the focus group will focus on the perception from computing students about phishing emails in general. The focus group will consider both the dialogue and the interaction (Kitzinger 1994; Smithson 2000; Halkier 2010; Grønkjær et al. 2011) and how meaning is co-produced in the group context (Wilkinson, 1998).

Questionnaire Design Process

The anonymised questionnaire will include an introductory section that will explain the participation of the study. The questionnaire data will be anonymised. The method of data collection in the questionnaire is to gauge policing and criminology students' awareness of different phishing attacks. McKenna and Bargh (1994); Spears and Lea (1994) stated that surveys completed anonymously lead to an increased level of self-disclosure (Lazar and Preece, 2001). It could be beneficial to understand the underlying factors in which why some students fall victim to phishing variants.

Paper-based questionnaires are completed anonymously from students are beneficial. Some benefits of anonymised questionnaires will make sure a GDPR (2016) clause is at the beginning of the questionnaire stating that data collected will be kept securely and used in a thesis without disclosing the participants' personal information. Another benefit of anonymised questionnaires is a higher response rate (Hanna et al. 2005).

The questionnaires were given to third year policing and first year criminology students in the School of Law, Policing and Social Sciences in Canterbury Christ Church University. They were selected because the study wanted to assess their existing knowledge about cybercrime in phishing specifically. The students' subject area might make them more knowledgeable about crime in general, but they may not be as knowledgeable about certain types phishing communication. The students in this group are ideal for this study because it will be interesting to see if they are aware of phishing communication which may be based on their prior knowledge. The results may indicate different awareness levels of phishing.

The results of the questionnaire were coded and analysed in NVivo 12. The information was coded by typing each students' response to a question in a Microsoft Word document and then categorising and coding students answers to a specific question to create statistical data in NVivo 12. NVivo 12 was used to analyse the questionnaire responses from a Microsoft Word document. A separate application called Numbers created some of the charts in the study.

The questionnaire design had a combination of open-ended and scenario-based questions. 9 questions in the questionnaire ensured the students provided a detailed response about their awareness and knowledge about phishing attacks they may have encountered in the past. It will then be beneficial for analysis later on in the study which may find a gap in knowledge about specific phishing attacks deployed by cybercriminals. Emails were sent to lecturers of policing and criminology and asked if their students were interested in participating in the study. Dates to visit the classrooms to distribute the anonymised questionnaires were when the teachers were teaching their lessons. I was present in the classroom when students were completing a questionnaire. It could increase the completion rate of the questionnaires. Also, students reassured by me that their responses are anonymised. It may increase self-disclosure from students about their awareness of phishing communication

Scenario-based questions were about a delivery company delivering an item with a small charge and encouraging them to click on a malicious link and a PayPal system error phishing communication. The purpose of the phishing email scenario questions was to find more information from the students about their understanding and awareness levels based on fictional scenarios they may encounter in their daily lives. It can enable the questions to gain an insight into their understanding and identify a gap in knowledge for these specific types of phishing fraud scams. Additionally, open-ended questions were about the security precautions that some students take against phishing emails and their variants such as 'SMiShing' (SMS phishing), Vishing, Spear Phishing and Pharming.

The purpose of security countermeasures open-ended question within the questionnaire was to understand the precautions that students might take against these types of phishing attacks from fraudsters. Moreover, another open-ended question was if the UK government was doing enough to make users aware of phishing emails and their variants. The question wants to gain an insight into the students' awareness of information provided by the government about different types of phishing communication. Another open-ended question was asking students what they would do if they received an email with an attachment. The purpose of this question was to find out if the students take the necessary precautions to check if an email attachment is malicious or not. The email attachment scenario question wanted to see if students take their time to thoroughly look through an email to check if it is a phishing email with a malicious attachment.

A spear-phishing email scenario question included general item information such as the order number and date purchased. The email asked the student to click on the link on the email to check the delivery progress of the item they had ordered online. The spear-phishing email question was assessing if students are aware of this type of phishing variant. The spear-phishing email scenario question did not want to deceive the participants and wanted their honest opinion about what they will do in that scenario. Another scenario-based question was about an email a student may receive when they made a purchase online during the Christmas period. The email included general item information such as the date of purchase and an order number. This specific type of Christmas phishing scenario-based question was an open-ended question that encouraged the students to share their honest opinion about what they will do if they receive this type of phishing attack communication from a cybercriminal. The Christmas phishing question wanted to see if some students would take precautions with the spear-phishing email and if students know it is a spear-phishing email.

The question design for all the open-ended questions encouraged the students to provide an answer to a question: 'If you answered Yes or No, please explain your answer or indicate that you are unsure below.' These options within the open-ended questions can enable me to gain an understanding of the awareness levels from the students about different types of phishing communication. Lack of knowledge of some phishing variants from the anonymised questionnaires will be questions about phishing communications. Mantzoukas (2008) noted that qualitative questions in surveys need three elements: content, coherence, and structure. Content is a question or area of interest explored. Qualitative questions are not interrogative sentences but are declarative sentences. The questions in a questionnaire will not be too focused or too broad. If some questions are focus on one area, the research will be inclined to follow preconceived ideas by creating leading questions (Lietz, 2010).

The questionnaire will have a combination of both open-ended and closed-ended questions. Open-ended and closed-ended questions can give an insight into the awareness levels from a specific student population of Criminology and Policing students and what they think they know about phishing emails and their variants. Phishing attacks are continuously evolving and are getting more sophisticated. Cyber-criminals learn new methods and are likely to change their strategies accordingly to defraud victims of their

personal information (Iacovos and Sasse, 2012, Kumaraguru et al., 2007, Kumaraguru et al. 2007). The questionnaire aims to address this factor and illustrate that phishing has become a severe cyber-security issue.

The difficulties of questionnaire design before a research study is the unpredictable nature of the questionnaire results. It is a bane of every researcher. There will different factors considered to gauge the awareness of students about phishing communication to overcome the barrier. A difficulty of wording a question about phishing variants is students that think about the stigma of being a victim of phishing and admitting to it. Students who do not admit to being a victim of phishing fraud may be part of a larger number of victims of phishing attacks. Also, the damaging effect it has on the economy. Another potential difficulty in designing a phishing questionnaire is the wording of the questions. The questions cannot be leading or make the students believe that they are being persuaded or pressured into providing a specific response to a question. Some questions can be interpreted or perceived as being too leading or narrow and can ask a student to answer in a specific manner. But this is avoided in the best possible way to avoid biased results and get purposive results to gauge the different interpretations of phishing communication variants from participants of the questionnaire.

It can be problematic when assessing the awareness levels of students from phishing emails. The questions need to ensure there is no stigma associated with their answers. The subject area about different phishing communication may worry students who do not want the stigma attached to being a victim of a phishing attack (Athanassoulis and Wilson, 2009). Students may claim they do not click on phishing links.

Some computing students may be peer-pressured which may influence the results of the focus group. On the other hand, studies found that they do click on links in phishing variants based on data collected by NCA, National Cyber Security Centre (NCSC), Action Fraud and various other voluntary agencies and police forces around the UK. One of the challenges of designing a phishing email and its variants questionnaire is cybercrime range from spam-advertised commerce, botnet attacks, malware attacks sent to users once they click on a link on a phishing email or a variant of a phishing message. Thus, it may be challenging to focus on specific phishing based on scenario-based questions and open-ended questions in the questionnaire.

One of the challenges of anonymised questionnaire design is: 'phishing usually occurs when a fraudulent entity is disguised within an email to illustrate that it is from an organisation's official email address and thus it will ask a victim for their personal information of their password' (FBI, 2017). Students admitting to clicking on a link on a fraudulent phishing communication variant can be challenging because of how the questions are worded and formatted.

Alternative data collection methods can provide useful insight into the different awareness levels of phishing variants from the interviews with students of the research project. For example, unstructured, semi-structured and structured interviews could be used as an alternative data collection method if the questionnaire results are different. All research methods have strengths and weaknesses. This study uses a mixed-methods approach to understand different awareness levels of phishing emails and their variants.

The purpose of the questionnaire design is to ask open-ended questions to explore the underlying factors in which why Canterbury Christ Church students have a gap in their knowledge about phishing attacks deployed by cybercriminals. Data collected from the questionnaire wanted to understand students' awareness levels of different types of phishing communication. Data from questionnaires found a gap in knowledge about zero-day phishing kits and certain types of phishing attacks from policing and criminology students. There was a visit to the classrooms to give the paper-based questionnaires to policing and criminology students when students had their lessons. It ensured that the anonymised questionnaires were completed and were not left to do later by the research participants.

A questionnaire was emailed to the ethics approval committee at Canterbury Christ Church University to ensure the study was compliant with GDPR (2016) and the Data Protection Act (2018). At the beginning of the questionnaire, there was a summary of the study and how data collected will remain anonymised. The study included information about the data collection methods used, how the data will be kept encrypted/secure at all times, how data collected is destroyed when the study has finished, and the study's purpose in the ethics approval committee form.

My university supervisors double-checked the ethics approval forms before submission to ensure the study followed the university policies. Students' identity was anonymous if they chose to participate in a focus group or anonymised questionnaires. The ethics approval letter stated that the study followed the university policies is in the (*Appendix-A pp.150-151*) section of this study.

The questionnaire encouraged students to explain their understanding of different phishing attacks by leaving some space beneath the questions so that students can write their answers. The limitations of questionnaires are the questions that only probe the students understanding on a surface level and do not explore the underlying factors into why policing and criminology students may fall victim to phishing variants. A limitation of the answers provided in a questionnaire is if the students have understood the question or read it carefully before answering a question (Hardré, 2006). An additional drawback of a questionnaire could be respondent fatigue. It means if the questionnaire perceived as too long by the students. The questionnaire could include questions that may be irrelevant to the student. A result of questionnaire taking fatigue can be when there is a low completion rate (Debois, 2019). However, a solution for this was the questionnaire focused on specific questions for the students to answer (Debois, 2019). Also, the questionnaire ensured that they were not too many questions for the students to answer. The questions in the questionnaire did not require the students to write a lot. Thus, improving the response rate of the questionnaires (Barrios, Villarroya, Borrego and Ollé, 2011; Kiernan, Kiernan, Oyler and Gilles, 2005).

Questionnaires gather statistical information from a specific population. It considered a beneficial aspect of surveys because representative samples are more reliable than small or non-representative ones (Kish 1965; Axinn and Pearce, 2006). The ease of web-survey software allows user-friendly data collection (Callegaro, Manfreda and Vehovar, 2015). Studies shown the advantage of text entries in web questionnaires enable participants to produce detailed responses. In comparison to self-administered questionnaires (Barrios, Villarroya, Borrego and Ollé, 2011; Kiernan, Kiernan, Oyler and Gilles, 2005). Online questionnaires are convenient for participants because they can answer the questionnaire at their own pace can be seen as an advantage when collecting reliable data from questionnaires (Callegaro and Wells, 2008). Online participants can view unsolicited communication, invitation to participate in online questionnaires are considered 'spamming' to participant in web-based questionnaires in a study (Harris, 1997). Online

questionnaires may have lower response rates than paper-based questionnaires. Thus, a paper-based questionnaire distributed to students in the study may have a higher completion rate (Hardré et al. 2006).

The questionnaire has a consent details section. The consent details section includes the title of the research study, my contact details if students have further questions. The final section of the consent details is how the data collected will be anonymised. There is background information about the research and what participants will be required to do. In a separate section of the study, there will be information about how data and personal information of the anonymised questionnaire are kept confidential and are compliant with the Data Protection Act 2018, GDPR (2016) and the University's data protection requirements. The questionnaire provided an opportunity for students to decide whether they want to participate in the questionnaire. The questionnaire has nine questions about scenario-based questions and open-ended questions about phishing variants deployed by cybercriminals. The purpose of the questionnaire is to understand their awareness levels, how students identify phishing communication from fraudsters and if students use security measures to mitigate phishing attacks.

Focus Group Process in the Study

Krueger and Casey (2000) believed that a focus group is less threatening to research participants. It was beneficial when there was a discussion about perceptions, opinions and thoughts about different phishing communication. The focus group aim was to moderate communication among participants. The goal of the focus group was to let the individual take the lead. As a facilitator, the discussion developed about a particular topic. Thus, as a facilitator, it was a marginal role. Questions prompted students to develop their answers about phishing variants. The focus group wanted to find how a group gives unique and similar responses to a particular topic about phishing.

The focus group uncovered aspects of understanding different phishing variants from students. There was a focus on the interaction between students themselves. The students provided a prominence to their views about different phishing variants scenarios they may have experienced or know that their family and friends had in the past. The

social context of the focus group provided an opportunity to witness the creation of meaning. It is through the interactions of participants in the group. The data generated from the interactive nature of the focus group offered insight. It would not be accessible exclusively from questionnaire data (Liamputtong, 2011).

Different scenarios about phishing variants in the focus group provided different layers of meaning from personal and public information. There was an analysis of the content of the focus group. It provided an insight into personal experiences of different types of phishing communication. The focus group identified the awareness levels of students and their experience of phishing variants. Different scenarios provided insight into how students think about different phishing variants. The phishing scenarios discussed in the focus group gave an insight into students' personal experiences of phishing communication. It allowed unique data collected from students. The focus group found the perceptions about phishing variants and the preventative security measures against phishing communication from the students.

The purpose of asking 'open-ended questions' within a focus group is to find as much information from the students about how they dealt with a vishing call and what they did afterwards. It allowed me to understand the participants thought process and if the right preventive measures against vishing. Open-ended questions enabled the students to share their personal experience with vishing fraud. Also, it allowed the students to listen and share further insight into their encounter with vishing. The purpose of asking open-ended questions may increase the possibility that students answer the questions about vishing in a detailed manner. It helped me to understand why students have been or had been a victim of vishing in the past.

The focus group wanted to collect anonymised information about first year computing students' knowledge and perceptions about different phishing communication and overall understanding of specific phishing variants. The focus group wanted to understand the underlying factors computing students may be defrauded by phishing variants when the questionnaire data is compared with criminology and policing students. Some students could know phishing related questions. Thematic questioning in a focus group could be fundamental to gauge their awareness levels of phishing variants. The questions in a

focus group can play a vital role in the research to know their awareness levels of phishing emails and their variants (Swaminathan and Mulvihill, 2017).

Computing students were picked as a data collection sample because the research study wanted to compare their understanding of phishing communication with policing and criminology students and find a gap in knowledge from a specific student population. The focus group was in October 2020. The computing students were in the first month of their computing course. It may have had an impact on their awareness of phishing communication.

The focus group was with first-year computing students. In the beginning, students were told about the anonymisation of their identity by following the GDPR (2016) and Data Protection Act (2018). Students consented to have their voice recorded in the focus group before the focus group started. The focus group as a methodological technique enabled me to find gaps in knowledge in some areas of phishing attacks deployed by cybercriminals. The group shared their encounters with phishing variants and how they took security precautions against specific types of phishing attacks.

Students did not specify how they can avoid being a victim of phishing when they discussed security countermeasures against phishing communication. The purpose of a focus group with computing students was to find out about their awareness levels of different types of phishing communication. Warr (2005) states that it can be difficult for some students to share their views if their opinions may be challenged and truncated as students join in or drop out of the discussions taking place in the focus group.

A voice recording Otter is used to record the students' voices in the focus group. The voice recording responses are in the data collection section of the study. It allowed me to find gaps in knowledge from the first-year computing students at Canterbury Christ Church University. The focus group questions were open-ended, and the students share their personal experiences of phishing emails and their variants. The questions were not leading and did not dominate the focus group; instead, there were opportunities for the participants to share their thought process if they received a phishing email or a phishing

variant and what they would have done in that situation. The following section will include further information about GDPR, confidentiality, data protection storage and ethics committee processes in the study.

Studies have found that the firewalls, encryption systems, authentication mechanisms or security certificates used by an organisation can be vulnerable to phishing attacks (Hong, 2012). It can be applied when students in the questionnaire if students fall for sophisticated fraudulent communications. A limitation of asking questions about different phishing threats is unanswered questions from participants who may not understand. Some students may provide an answer to question-based on their prior knowledge of phishing variants. Students asked to identify phishing emails may not represent the actions of real-world users. They are not reminded occasionally about the risks of phishing emails in real life (Parsons et al., 2015).

The focus group covered the following topics: *Scenario-based discussion asked about PDF document attachment from a University Lecturer, Vishing Fraud, Smishing, Phishing communication from fraudsters, Prevention of Phishing Attacks and Protection against phishing attacks*

Focus Group Data Collection

A method explored in the study is a focus group. A focus group is when students in an informal setting discuss their experiences of different types of phishing communication distributed by cybercriminals. The facilitator in the focus group ensures students are focusing on a topic. Detailed answers from computing students can gauge their knowledge awareness of phishing variants (Clifford et al., 2016). According to Kitzinger (1994), focus groups can be complementary. It means that students can share their experiences, concerns and needs. The focus group will be with computing students to gauge their awareness levels of phishing emails and their variants. Data collected in a focus group compared with the questionnaires.

Promoting discussion is essential in a focus group. Questions in a focus group may help to elicit comments made from an individual. Interpretative phenomenological analysis can understand what a person is thinking about from their perspective (Larkin et al. 2006). Questions and topics mentioned at different stages of a focus group can make analysis difficult because it requires trying to relate responses in various contexts and times (Lazar and Preece, 2001). Mantzoukas (2008) found the importance of research findings has value only if they provide clear answers to well-structured questions. A poorly worded question is unlikely to lead to another unrelated question linked to an issue. It can be associated with a focus group whereby effective questioning is fundamental because it can gain an insight into gauging awareness levels of phishing emails and their variants.

A focus group is useful for understanding perceptions of phishing emails and their variants because it can provide an opportunity to evaluate interactions between participants and find out the underlying factors in how meaning is constructed collectively and shared. Different perspectives from students in a focus group will uncover underlying factors to extract information from them (Kitzinger 1994; Bryman 2008; Liamputtong, 2011). Information extracted during the focus group is awareness levels of phishing emails from different people. The focus group can show different awareness levels of phishing emails and their variants from the computing students.

A method used to analyse focus group is discourse analysis that probes a conversation in search of cues that may provide a deeper understanding of phishing emails and their variants (Sharp, Rogers and Preece, 2007). Discourse analysis is a qualitative and integrative method to analyse text. It differs from systematic and content analysis. Discourse analysis used to focus on knowledge of phishing from students in the study. Discourse analysis used to consider the different ways language presents different understandings of a phishing variant discussed in a group discussion. Discourse analysis used to examine written and spoken text in the focus group (Paltridge, 2006). It was analysed and reviewed using a voice recorder app Otter was used to gain detailed written notes from participants in the focus group. An Otter app in a focus group assessed the knowledge of phishing variants is weakest from computing students. The computing students' knowledge about phishing attacks awareness and their understanding by using discourse analysis as a process. Discourse analysis will review an entire conversation and written transcript in the focus group.

A group discussion interprets students' knowledge and awareness about phishing variants when students discuss their understanding of different phishing communication from cybercriminals in a focus group. Introductory remarks at the beginning of a focus group will outline how the focus group process will occur, including encouraging them for an honest, open, respectful dialogue that everyone can inclusively participate. In a focus group, the questions can and answered by anyone, and those who have a different opinion from another person will be able to share their opinion as well (Berg and Lune, 2012). Hennink (2014) found people share different perspectives and experiences on specific topics in a focus group. It will result in diverse responses recorded about phishing variants and what the participants do base on their personal experience.

Opening questions asked in a focus group about specific topics about the research. General questions about phishing communication may allow the students probed for complete answers and encourage them to answer questions conversationally. The use of probes during a focus group is fundamental because it will keep the group focused. Students guided to the main discussion points of a group discussion. Further questions about phishing used to seek clarity from their knowledge and awareness of phishing. Questions about phishing variants to answer in a focus group can lead to an insightful discussion about different types of phishing attacks. It is a vital aspect of a focus group because data collected will be generated for analysis from students' responses. The questions at the end of the focus group will be more general and provide closure to the focus group. There will be a summary of the key points covered by students. Further questions ensure that their opinions are accurately reflected (Aurini, Heath and Howells, 2016). Overall, focus groups can be beneficial when using group dynamics to generate qualitative data.

Limitations of transcription from the focus group are words missing, odd phrases, incomplete sentences, half-finished thoughts and other characteristics of spoken word in a group discussion. These characteristics are associated with the flow of a conversation, but they may make it difficult for a reader to follow the notes. Notes are re-worded to ensure the sentences grammatically correct. An aspect of a focus group is an understanding of how participants communicate. There must be a consideration of a particular topic discussed. Transcription of a focus group should not be edited excessively and changed even if students use poor grammar or confused about a topic discussed in the focus group (Stewart, 2006).

Nevertheless, survey findings may result in contradictory results. Thus, focus group discussions can be used after quantitative research from questionnaires to gain contextual information from the anonymised data used to provide examples to support quantitative findings in a focus group. Focus group data can enable refined explanations about topics covered with participants and may challenge how the data interpreted at the end of a focus group (Liamputtong, 2011).

Structured interviews were not in the study as a form of the data collection method. Structured interviews require participants to answer pre-determined questions prepared before the interview. The data analysis for structured interviews can enable differences and comparisons made from questions asked and answers given in an interview (Boyce and Neale 2006). Structured interviews include closed questions, and they would follow a pre-designed question. Results of a structured interview will be generalised, and the hypothesis tested at the end (Bowling and Ebrahim, 2005). Structured interviews were considered at the beginning of the study but discarded because after criminology and policing students completed the questionnaire, they did not want to do an interview.

A paradigms approach is not in the study. A paradigms approach uses cross-validation to analyse data collected in the focus group and questionnaires (Sale, Lohfeld and Brazil, 2002). It is a limitation of the study in terms of data collection because a paradigms approach was not a data collection method. Data collection can be in-depth in cross-validation and allow strategies developed. It can reduce the chance of victims defrauded from different types of phishing communication methods used by cybercriminals. The paradigms approach in research based on a different perspective of reality. The use of cross-validation can enable the gauging of awareness levels from students from phishing emails and their variants. Moreover, it can allow data collection to be in-depth and develop strategies to reduce the number of victims defrauded from different phishing communication methods used by cybercriminals.

Philosophical approaches from a theoretical perspective are interpretivism and inductive research. Students' views considered from a focus group and questionnaires (Creswell and Clark, 2007). Some aspects of subjectivism used as critical inquiry in a focus group about phishing emails and their variants. The focus group content is analysed and used as statistical analysis. Mixed methods research philosophical foundation is on a worldview approach (Creswell and Clark, 2007).

First year Criminology and third year Policing students in the School of Law, Policing and Social Sciences at Canterbury Christ Church University are the sample size chosen for the questionnaires. The study did not focus on different departments that can provide insight into students defrauded from phishing attacks. A majority of students may not want to do interviews after completed the questionnaire when prompted at the end of it. It can be due to numerous factors. A potential challenge of questionnaire research enough people are responding to the questionnaires (Lazar, Feng and Hochheiser, 2015). The limitation of a focus group and questionnaires is students need to recall their perceptions and experience of a specific topic. Thus, they mention what they remember (Lazar, Feng and Hochheiser, 2015). The anonymised data collected from the focus group with computing students in Canterbury Christ Church University found that some students experienced phishing attacks from fraudsters in the past.

As part of exploratory research, the design is to gauge awareness levels of phishing emails and their variants based on addressing potential research problems. There are strategies implemented to address these challenges. Whether chosen data collection methods could have equal or unequal weighting and how the data collection methods are mixed. A rationale to use quantitative and qualitative data can find where the awareness of phishing attacks is weakest within the research study. The qualitative data and their analysis explain and provide statistical results. It will explore students' view about phishing variants in more detail and explore the underlying factors which why they are victims of phishing attacks (Rossman and Wilson, 1985; Tashakkori and Teddlie, 1998; Creswell, 2003).

The data collected from the focus group can use an interpretivist approach. An interpretivist approach could assess the awareness levels of policing students who may know about law enforcement agencies that can block specific domains or websites that source malware using Domain System (DNS) blocking/filtering. It can prevent phishing activity that uses domain 'spoofing' when an email appears to be from a specific sender such as a bank or government department, but it is fraudulent. An interpretivist approach can understand if students are aware of prevention strategies. Prevention strategies protect users from email verification systems within government networks, online banking, other websites reduce the possibility of people defrauded by online fraudsters (National Security and Intelligence et al. 2016).

A study carried out by Sheng et al. (2010) found that phishing education can help reduce users' tendency to become victims. Educational initiatives can increase phishing awareness (Arachchilage and Love, 2013; Arachchilage and Love, 2014). Phishing threats can have negative consequences for victims who may receive different types of phishing communication sent by fraudsters. Educational training sessions might provide the skills to reduce the chances of university students victimised by phishing variants. Recent research has shown education as a strategy for intervention against phishing variants can decrease vulnerability amongst users (Qabajeh et al. 2018; Alsharnouby et al. 2015). Similarly, studies found knowledge and suspiciousness about phishing communications could reduce the chance of both younger and older adults defrauded from phishing variants (Nmachi and Win, 2021). The results section of the study will explore the different types of phishing communication and considers educational initiatives based on the results. The results section will answer the following research questions: *Research Question 1: What are the underlying factors in which students fall victim to different types of phishing attacks?* This will be explored and analysed from the anonymised questionnaire results. *Research Question 2: Does the perception of different types of phishing emails from students correspond with statistical information in a focus group and anonymised questionnaires?* The perception of phishing variants will be explored from the questionnaires and the focus group with computing students.

Results

The focus group was with six first year computing students. Six students picked from random sampling. All of the computing students allowed to take part in the study. The effect the selection method made on the results from these students is not being selective on students existing knowledge different phishing communication. It made the results unbiased because the computing students are picked at random. They were asked different questions and were allowed additional time to elaborate on specific phishing communications in a group discussion. Computing students are given a brief description at the beginning of the focus group about the study and what it entailed. At the beginning of the focus group, students made aware that their identity remains anonymous, and data collected for the study will be anonymised and kept confidential. A choice is given to students if they are not happy to participate at the beginning of the focus group can leave the focus group. Students made aware that there is no right or wrong answer, and no one will judge them if they do not know about a specific phishing attack. It put the students at ease and made the focus group discussion flow nicely. The first year Computing students from Canterbury Christ Church University helped each other with the questions about phishing attacks and learn from each other about the potential threat phishing poses to them and the general public.

The second section of the results section of the study was questionnaires. Questionnaire results found the different awareness levels of phishing variants. The questionnaire results focused on both '*Research Question 1 and Research Question 2*'. Some policing and criminology students identified the risks phishing communication may pose to themselves, their friends and family. They were given the questionnaires at the beginning of the lecture and given 15 minutes to complete it. The number of anonymised questionnaires collected was 177 students. It was broken down to 100 (56%) the third-year policing students and 77 (44%) criminology students who completed the questionnaire. It was due to the ease of sampling of students. The results could have looked at the broader Canterbury Christ Church student base from students in other facilities about phishing variants. For instance, the questionnaires could have looked at students from other departments.

The study has a limited sample size compared to UK government studies that do nationwide surveys within England and Wales about phishing attacks. This study focuses on a specific student population. It achieved this well. However, there were some limitations to this. The demographics of students in Canterbury Christ Church University has 15,000 students (Canterbury Christ Church University, 2020). The current study can be generalised for other students in other university which can gauge their awareness of phishing variants.

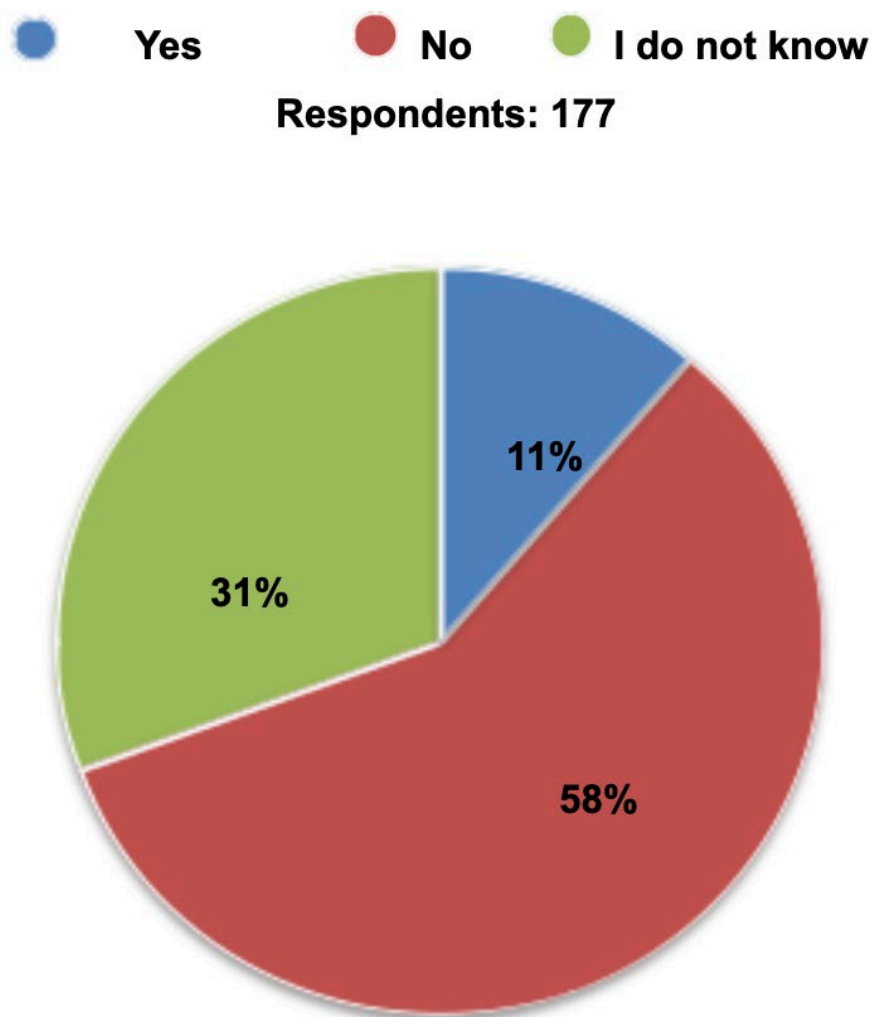


Figure 1: Result of first question in the questionnaire: *Is the government doing enough to make users aware of phishing emails and their variants?*

Students asked about UK government websites making people aware of different types of fraudulent emails, text messages and calls from fraudsters. In (figure 1) 58% of students (103 students) said that UK government websites do not provide enough information and make people aware of different phishing variants. These results were from the School of Law, Policing and Social Sciences in Canterbury Christ Church University. 31% (55

students) were not sure about phishing variants or were not aware that there is information about phishing emails and their variants on different UK government websites. Only 11% (19 students) of university students agreed that there is information about phishing variants and precautions taken against social engineering tactics deployed by cybercriminals. The results found that people should be more aware of different phishing variants on UK government websites to find information about social engineering attacks.

Data sampling: Focus Group and Anonymised Questionnaires

The questionnaire data collection sample was with policing and criminology students. The focus group was with computing students. The knowledge and awareness levels of taking precautions with phishing attacks from cybercriminals from the two groups are mixed. Results may be suggesting that there were areas when the knowledge of students was weakest for some phishing variants. Some students struggled to explain the security measures and the identifying features of different types of phishing communication. The link between policing, criminology and computing students based on their mixed understanding of phishing communication from fraudsters is explained further in this chapter. The study wanted to compare policing and criminology students understanding of phishing communication from questionnaires with a focus group with computing students. A reason for this was to assess the computing students understanding of phishing communication in more detail by using a focus group instead of a questionnaire.

The anonymised questionnaires sample size of 177 students which is a sufficiently large sample size. It is an effective sample size of policing and criminology students in Canterbury Christ Church University. But it is not a significant number when generalising the UK student population. However, the study wanted to carry out data collection from a specific population of students. Another limitation of the data collection sample from the anonymised questionnaires is it focused on a specific university department: School of Law, Criminal Justice and Policing at Canterbury Christ Church University. The study could have looked at different departments and how they respond to phishing communications and how students may have suggested security measures against phishing variants. The study wanted to look at a specific university department initially before analysing data from other departments.

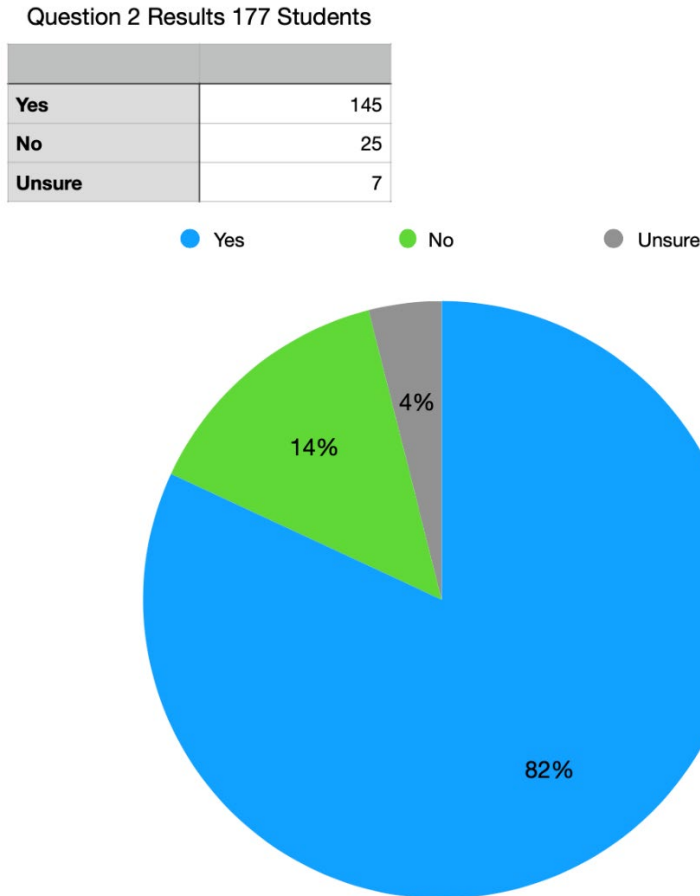


Figure 2: Result of second question in the questionnaire: *‘You have received an email from a purchase you have made online for an item you have ordered during the Christmas period. The email contains general item information such as: the order number and date purchased. The email advises you to click on the link on the email to check the delivery progress of your item. Would you click on the link?’*

There was an example of a spear-phishing email scenario (see figure 2) that included general item information such as the order number and date purchased. It was the second question in the anonymised questionnaire. NVivo was used to analyse the data. The ‘Numbers’ application created the pie chart. The same data analysis methodology made all of the charts in the study.

82% (145 students) will click on the link to check the progress of their item. It suggests that they may fall for this type of spear-phishing email. There is a detailed transcript of the students’ responses to the second question of the questionnaire (See Appendix E for detailed transcript of student responses pp.165-174).

Results (in figure 2) found that 145 students (82%) answered 'yes' shows in the Christmas phishing email scenario they may get defrauded. Of those surveyed, only 25 students (14%) answered 'no' do not click on the link within the email. There is a small portion of students who may not be a victim of the phishing attack. One student said no, and the link could contain malware that can steal their personal information or carry out malicious activity. It demonstrated that the student considered the cybersecurity risks associated with some emails might be phishing email can contain malware (Satpathy and Mohanty, 2020). Another said no because the student usually signs up for text notification to alert them if their item has arrived. The student's response may imply the student identifies the email as a phishing email and suggests getting order updates via text. A student said the email that they received would appear to be a phishing email. However, the student did say the reasons why the email is a phishing email. It does not show their awareness levels of the phishing email. Other awareness which was sought was the identifying features or content of a phishing communication. The rest of the students (4%) 7 students answered, I am not sure. 4% of students might not know anything about phishing emails.

Interestingly, a student said that:

'I wouldn't just randomly click on an email I would look at who it has been sent from to check its credibility-if I was unsure, I would just leave it'.

It illustrates that the student may check if an email was genuine and then deciding to click or not to click on the link. However, the student did not explain if an email was a phishing email how the student would identify it as one and check its credibility.

Students were asked if they received any phishing emails and then asked to explain how they identified the email to be a phishing email. The results of the third question created mixed responses. 98 students said yes, 32 said no and 47 students were not sure if they have or have not received a phishing email. From the 98 students a student said that:

'It is hard to identify them, banks etc will always write to you if it is important so any emails from banks, HMRC etc I always ignore'.

This assumption of the student that banks or HMRC will always write to the recipient is not correct. The student said that phishing emails sent to people are from banks and HMRC. This statement from the student is not correct. Different strategies to send phishing emails from fraudsters can encourage people to click on the link. For example,

to check the status of a library book they had borrowed. The student has not considered precautions taken if an email appears to be a phishing email.

The question results asked if students received a phishing email. The results showed that some students do not know the difference between a spam email and a phishing email.

Student (7): 'It just looked fake; I mean wow I've won an iPhone X from Aldi? yeah right'.

Student (9): 'Emails claiming that I have been in a road traffic accident, emails saying I have won in a competition and need to enter details to receive the prize'.

These examples of generic spam emails sent to numerous recipients with notification they have won a prize or involved in a road traffic accident. Students may have misinterpreted the difference between a phishing email and a spam email. There appeared to be confusion or lack of awareness to identify the difference between phishing emails and spam emails. Some students thought that unsolicited spam emails sent to multiple emails and individuals with phishing emails.

Students who said they were not sure on how to identify a phishing email response were:

Student 1: 'I tend to ignore dodgy emails, so they may not be phishing, but they also could be'

Student 2: 'I wouldn't know, hope not'

Student 3: 'Cannot identify'.

From the questionnaire results three answers frequently appeared as an answer: 'I do not know'. They 'cannot identify a phishing email' and 'assumption that a phishing email will always be sent to the junk section of their email' These students are more likely to be victims of social engineering attacks because they do not have enough awareness and knowledge about different types of phishing variants.

Another concerning factor when the students responded as: 'I do not know'.

If they check emails which appear to be important and open emails if they are expecting a reply from someone. This can result in them either opening or downloading unknown attachments or opening links within an email because they may not check for elements in the email which could identify it as a phishing email.

A scenario-based question was assessing whether the students will be a victim of a smishing text message or not. Some students said they will click on the link to read through it or find out what it is about.

Another student said:

Student 15: 'Open the link to check that it is legitimate. Check that there is the lock on the left-hand side to make sure it is secure'.

The student did not consider once clicking on the link they may have their personal information stolen and might become a victim of identity theft or have a spyware, malware and a trojan virus installed on their mobile phone to either steal their personal information or use their mobile phone to connect to a zombie bot network to launch cyber-attacks such as Distributed Denial of Service attacks (DDoS) attacks without their knowledge (Terranova, 2021).

A student might have based the legitimacy of a link in a text message if it appeared encrypted by showing a lock icon in the URL. It shows the student will click on the link can result in having their personal information stolen. Also, the student may be lacking a basic level of online safety awareness (Furnell, 2007), and they react to trust indicators which in this case was a 'lock icon' (Jakobsson et al., 2007). Moreover, hackers may generate a fraudulent link that appears to be encrypted to steal their debit-card or credit card information in a smishing text message.

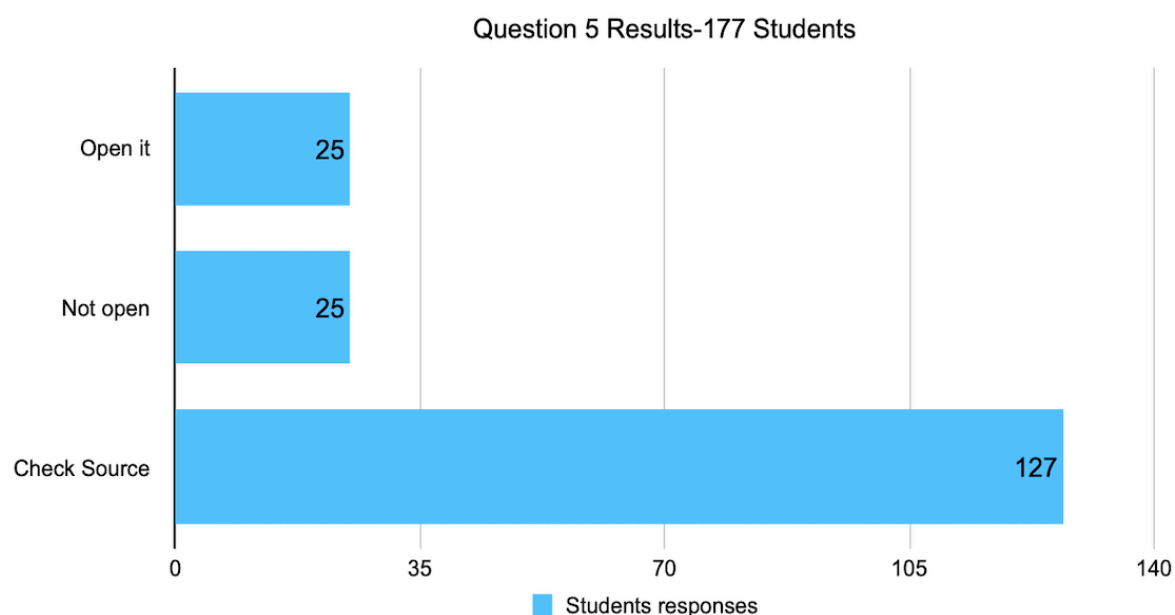
Some students said they click on the link to pay the delivery fees:

'Pay the delivery fee'.

'Pay it to prevent any hassle of getting my parcel. I would rather pay to receive it at a specific time then wait to get it'.

'Click on link check if link is same as actual FedEx website if it is then pay fee'.

The students can have their personal information stolen when they will click on the link. These students said they wanted to check if the delivery website looks official. Some students may enter their card details to pay for the delivery fee. These students could be victims of a smishing text message fraud.



(Figure 3) Result of fifth question in the questionnaire: *What would you do if you receive an email with an attachment?*

The fifth question in the questionnaire result was mixed. The majority of 127 students (83%) said they check the source of an email attachment. The majority of the answers stated they would open attachments if they recognised the sender. The results indicated that they are more likely to check attachments are malicious or not. The answers given about the email attachments were vague and did not specify how the students may check attachments are malicious. Most of the responses were:

Student 1: 'Depending who it is from, I would open it'.

Student 2: 'I would check the email, depending on who it is from I would view the attachment.'

Some students may be defrauded from spear-phishing emails when cybercriminals use tactics to persuade them to download a malicious file attachment. Spear-phishing attacks are targeted attacks and use information about a target to make the attacks more specific and personal to the target (Phishing Tackle, 2021). It could make some of the students vulnerable to spear-phishing emails when most students said they open attachments from someone they trust (See *detailed transcript of student responses for question 5 in Appendix F, p.174*).

7% (25 students) said they open the attachment in an email. Some examples of the responses were:

‘Open the attachment’.

Open the attachment, only if PDF’.

Some students may not identify or explicitly said they would check if the email with the attachment is a phishing email. Some even said they trust a PDF file format as an email attachment regardless of who sent the email. It is worrying because a phishing email attachment may contain malicious malware variants such as viruses, worms, trojan horses, spyware and adware when opened or downloaded onto their electronic devices. The malicious network content may enter the students’ electronic devices when they open a phishing email.

Examples from students who will open an attachment:

Student 1: ‘If it’s a PDF document’.

Student 2: ‘Generally, open it as it most likely may mean something-they can’t hack me from opening an attachment.’

These statements from the students are untrue. Students may not have known that cybercriminals can hack their electronic device if malicious attachments are open. Students could consider a PDF email attachment is harmless once opened from an unverified sender in a phishing email. The students may not know that PDF attachments contain embedded malicious executable programs. Students may not be aware that some PDFs can have a virus or hidden malware (Abraham, 2021). Also, the attachments may contain malicious content that may be in PDF files can infect different files through a variety of malware attack vectors: JavaScript, a system command, hidden objects and multimedia control (Amin et al., 2013). JavaScript in websites coding is to control browser appearance and functionality. Vulnerabilities are exploited in Adobe to carry out malicious activities. A PDF attachment can open a command window and execute commands to initiate malware in system commands. Hidden and embedded objects in PDF attachments are encrypted. Embedded and hidden objects can make detection difficult for anti-virus scanners. Hidden objects execute malicious commands when a PDF attachment is open in phishing email variants. Multimedia control is when some malicious PDF attachments have embedded and hidden objects that could be a QuickTime media or flash file. Cybercriminals can exploit vulnerabilities in media players (Abraham, 2021).

Some anti-virus software may have limited effectiveness when scanning files or phishing email attachments for malicious content against different exploits from polymorphic malware attacks. Polymorphic malware can defeat the signature match by mutating itself while keeping its original malicious capabilities intact (Rad et al., 2011). Malware signatures from attachments generate one form of a polymorphic virus that may not match against a mutated form (Rad et al., 2012). Thus, polymorphic malware is known as multiple viruses rather than a single virus. Anti-virus software which identifies polymorphic malware variants is desirable. Most anti-virus software cannot detect these (Fraley, 2017). Naidu (2018) found that modern anti-virus systems cannot detect new polymorphic malware variants even if the signatures match with one or more variants belonging to a specific polymorphic malware.

One of the issues with detecting malware variants within attachments is malware detections systems may not detect malware without a password. Malware detection systems can find it challenging when scanning encrypted content from hackers. The result of the questionnaires indicated that students are enticed to open and decrypt the attachment, thereby executing malicious executable or other malware variants within a student's device/devices. It is because malware writers who attach encrypted attachments in phishing emails can make detection from anti-malware systems difficult. Malware writers rely on a social relationship between the 'sender' of the email and the recipient to make it appear safe to open an attachment. The attachment content uses deceptive tactics to trick the recipient into believing it is safe to open an attachment without consequences. It was the case when some of the students in the anonymised questionnaire said they open an attachment in an email (Amin et al., 2013).

Student (7) said that if they receive an email from someone, they do not know they would not open an email attachment but if an email attachment appears to have been sent from a family/friend or an official company they will open the attachment:

Student (7): 'If it's from someone I don't know, I wouldn't open it as I don't trust them. But I would open it if it's from a family/friend or an official company'.

Student (7) may not be aware that cybercriminals can send phishing emails that appear to be from an official company or sent from family or a friend. The student could be a victim of a phishing email in the future because the student did not stipulate in their response to the question that they do thorough checks even if the email is supposedly from their family and friends or an official company. Recipients who open attachments from an email without checking the content of the email and verifying its legitimacy may lack the security awareness required to protect them against phishing attacks.

In contrast, 25 students (8%) stated they will not open the email:

Student (1): 'Don't click on the attachment until you know it's legit.'

Student (2): 'Do not click on the attachment.'

These responses to the question illustrate that 8% of students might check the source of the email. It shows the students are slightly more cautious when they got an attachment from a person in an email. Students said they either ignore an email or open it. But they did not specify the underlying decision-making process about why not to open the email attachment.

Student (11):

'Depends where it's from. If I didn't expect to get it I'd ignore/delete'.

Most people do this when they get a phishing email. They delete phishing emails or are relying on the spam filter embedded in their emails to filter malicious emails (Yu, 2020).

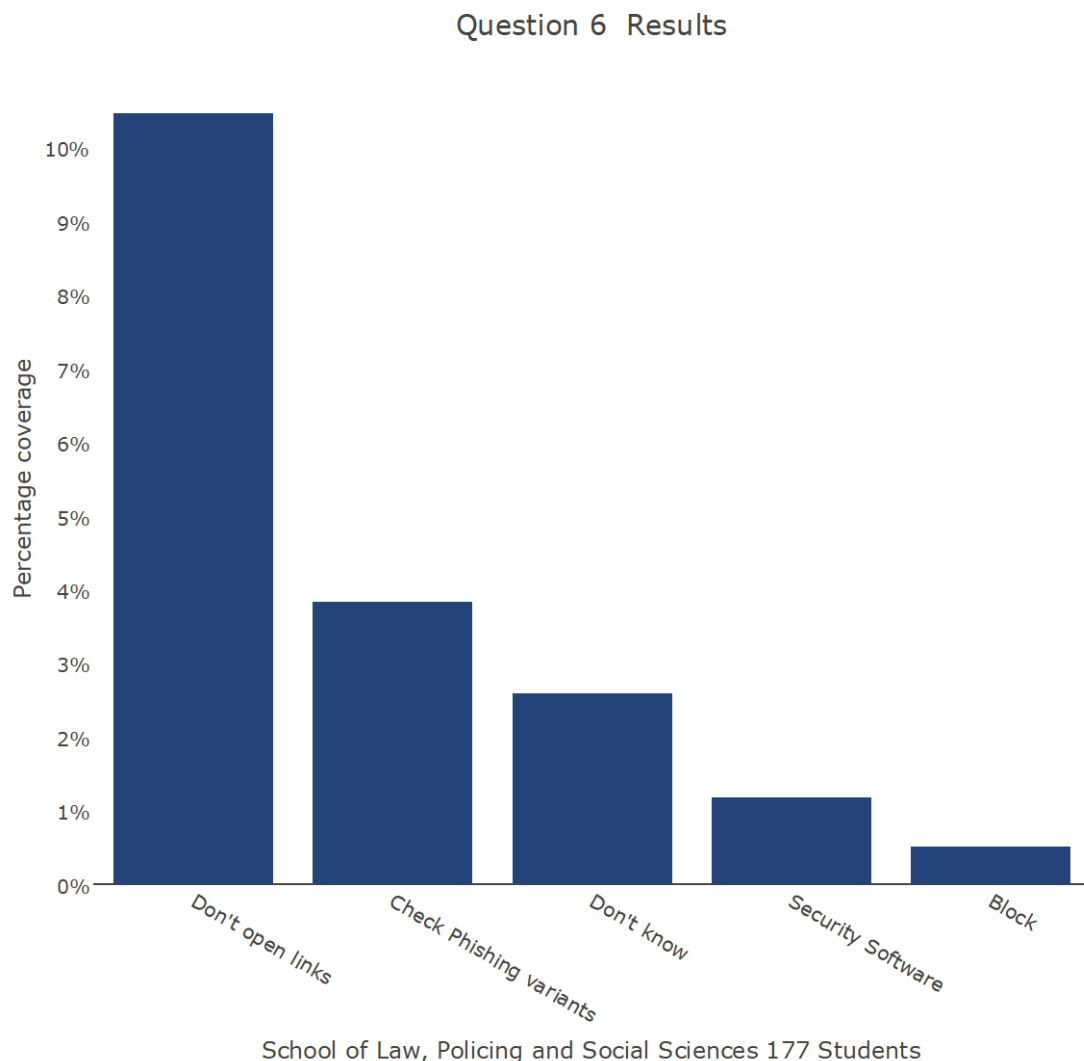
Student (10):

'Depends where it's from'.

The student (10) may be vulnerable to the personalisation of spear phishing attacks that can lure a student divulge personal information because it is seen as less suspicious compared to spam phishing baits due to their target approach. The nature of sophisticated spear-phishing emails can make them difficult to detect. A spear-phishing email careful design and timing of a message should make it possible for a user to click on a link. A user may be intrigued about something, interested in the message's content and context.

For example, the phishing message might come from a known sender (Benenson et al., 2017).

The results presented in the bar graph (below) shows the most common responses provided by criminology and policing students. Students' precautions taken avoid phishing emails and their variants: SMS Phishing/Smishing, Vishing, Spear Phishing and Pharming.



(Figure 3) Results from question 6: *What precautions should you take to avoid phishing emails and their variants: 'SMiShing' (SMS phishing), Vishing, Spear Phishing and Pharming?*

The majority of students did not suggest anti-virus and anti-phishing browser security toolbars to detect a phishing website domain when visited by a user. Only 1% of students (2 students) in the questionnaire stated that they use security software against phishing variants. Again, it can make the students vulnerable to different types of phishing

communication that may contain malware. 11% (19 students) of the students said they don't open links from phishing variants. It is worrying as the remainder of the students may be defrauded from phishing emails and their variants if they open links. Another worrying aspect of the results is that 4% of students (7 students) said they check phishing variants which means that 96% of students (170 students) may not check phishing variants when they receive one. (See Appendix G, Question 6 Students Response Data pp.182-190).

3% of students (5 students) responded 'do not know' what to do if they received a phishing communication.

Some students who did not know what the phishing terms meant said:

Student 111: 'I don't really know what phishing means' 'Never heard of any of them'.

Student 99: 'I don't know...Never been taught or told'.

Student 66: 'Not sure'.

Student 70: 'I don't know'

Student 15: 'Unsure, maybe avoid entering your email address into websites unless needed'.

The result of the question found students who were not aware of phishing emails and their variants and the precautions they should take is worrying. They are more likely to be defrauded by cybercriminals from phishing variants. Results of the question found some students may not be aware of phishing variants. They do not know how to identify phishing variants and precautions they should take to avoid phishing variants. There could be a possibility that students are not familiar with the terminology used to describe the different type of phishing variants and thus are unable to explain security measures to be taken to avoid them. The students who were unsure about what phishing attacks mean may not educate themselves or educated from phishing training sessions about the latest cyber threats from social engineering tactics used by cybercriminals to defraud victims.

A student suggested security measure such as:

'Have a better security software like a VPN'.

It does not necessarily prevent phishing variants because they can bypass security measures such as a VPN or if the victim clicks on a link on an SMS phishing that can potentially install spyware or malware on their mobile phone.

Other precautions that students suggested in the questionnaire was:

Student 13: 'Create a spam folder for emails'

Student 33: 'Have different passwords for different accounts. Put them in spam so they only appear in junk' and 'Spam filter, change email received settings'

These precautions can reduce the number of spam emails received in their email inbox but not phishing emails. The students failed to understand that even if they install a spam filter or have different passwords for different accounts' it does not act as a precaution against different phishing variants. Additionally, spam filters may find difficulties detecting image spam because it executes a range of image creation and randomisation algorithms. In image spam, the text message is embedded into attached images to bypass anti-spam filters. In Image spam an obfuscating method in which the text of an image is stored as a GIF or JPEG image and displayed in a phishing email. This prevents text-based spam filters to block the malicious email (Ismail et al., 2019).

Moreover, a student said that having different passwords for different accounts can protect the user's accounts. But this not the case for malicious phishing emails and their variants. A student's security measure for having different passwords is ineffective against some phishing variants. Some phishing communication may deploy spyware onto a victim's electronic device once an email attachment downloaded or a link clicked on in an email can steal their passwords of the individual users on their accounts. Other phishing variants create a login web page that is a replica of a target organisation include images and the logo sent to a user in an email message, requesting them to log in to keep their accounts active. Thus, this may compromise a participant's different passwords on their accounts. Some cybercriminals send an email with a link to the login page hosted in a fraudulent server. The fraudulent login page hosted at a URL (Uniform Resource Locator) matches the original, genuine login page. There is a slight difference in the domain name that rarely is identified by a user (Shaik, 2020).

Student (7) said to create a spam folder for emails but did not state the features of different phishing attacks. The student did not mention how to identify phishing variants. Creating a spam folder does not act as a security measure to protect the respondent against phishing attacks.

Other students suggested to:

Student (3): 'Avoid dodgy websites block the number/email as soon as receiving redirect unknown emails to junk'.

Student (114): 'Don't go on random sites and input personal data'.

Student (93): 'Block emails and text if this carries on then keep blocking and ignoring'.

Student (172): 'Not giving out email/ number to unknown sources'.

Student (32): 'Don't give out your email, phone number to random people and select no when they ask to pass your details onto other people'.

Providing personal information on questionable websites and providing sensitive information to other people can lead to phishing variants to be received which is identified from the students. The answers did not expand on why personal information should not be entered on 'random sites' which does not show if they know about the precautions need to undertake against different types of phishing communication distributed by fraudsters. Some of these suggestions are not precautions for different phishing variants such as avoiding phishing websites does not prevent phishing variants as well as blocking emails and text continuously does not act as a precaution to phishing variants because the participants did not state the precautions which needs to be undertaken to avoid different types of phishing variants.

The limitation of browsers which blacklists phishing URLs is that the phishing URL has to be previously included in the blacklist. Thus, the participant will still need to be cautious when they visit certain websites which can be phishing websites. Participants may have not been aware of the security precautions which can be taken against some types of phishing emails. There are some machine learning systems which can be used by users to detect phishing such as: streaming analytics, neural networks and support vector machines. However, a drawback of these machine learning systems which detect phishing by deleting or adding the features extracted from the email is it can be time-consuming because the features are manually selected which is one of the limitations of machine learning techniques, and Deep Learning which is a subfield of machine learning requires a vast amount of data for better results but does not need manual feature engineering and can detect new phishing URLs. Also, the increased sophistication of malware variants used in phishing variants can bypass security mechanisms (Nmachi and Win, 2021). For example, the limitations of blacklists that use a heuristic-based approach detect newly phishing websites which blacklist is not able to do (Abdelhamid et al. 2014), and the ability of heuristic-based improved the rule-based method of detecting phishing attacks. The rule-based approaches perform well on set rules, but they do generate high false alarm rates. The rule-based approaches in machine learning need a user to update set rules for a vast amount of data which is a challenge to this approach (Xiujuan et al., 2019).

Malware authors who launch phishing attacks use communication channels hidden within network traffic. They are benign and difficult to block. The domain names that host the command and control (C and C) server change domain names. Domain Generation Algorithm (DGA) generates millions of pseudo-random domain names. The compromised devices will attempt to connect to be provided with new commands, making blacklisting methods useless. The botmaster use of fast-flux to change IP addresses can make takedown mechanisms used against malicious phishing domains challenging (Yue and Wang, 2008).

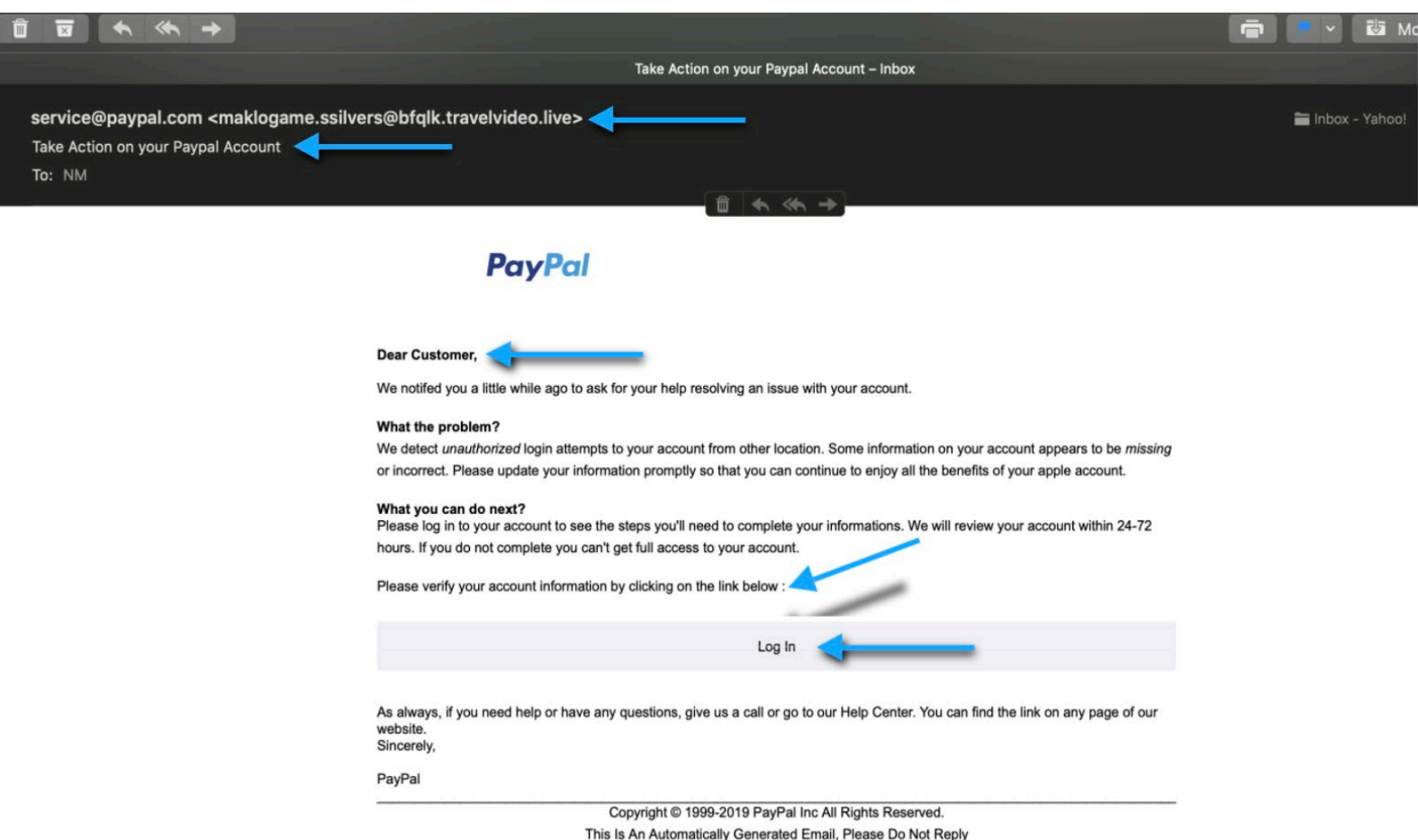


Figure 4: Malicious phishing email with the purpose is for the theft of personal information from victims who may have a PayPal Account

(Figure 4) shows an example of a malicious phishing email with the purpose of theft of personal information from victims who may have a PayPal account. The blue arrows show the identifying features of some phishing emails. This email identified as a phishing email from the fraudulent 'from address'. The email has a generic opening of the email 'Dear Customer' email asks the recipient to verify my PayPal account information by clicking on a link. Additionally, the email subject has a sense of urgency about the PayPal account: 'Take Action on your PayPal Account'. The content of the email states an issue with the PayPal account. There have been unauthorised login attempts from another location, and there is information missing or incorrect in the PayPal account. These are all features of a phishing email that may not get identified by some users who do not know how to recognise a fraudulent email.

The majority of the students said that they will contact PayPal by calling them directly:

Student 1: *'Contact PayPal myself to check the accuracy of the email'.*

Student 2: *'Contact PayPal before doing anything in the email'.*

Student 3: *'Contact PayPal or cancel/freeze the card attached to the PayPal account'.*

Student 4: *'Call PayPal helpline to sort the problem directly'.*

Student 5: *'Ring them and ask for a full explanation'.*

Student 6: *'I would call up PayPal customer services to figure out what is going on'.*

Student 7: *'Ring them and ask for a full explanation'.*

Student 8: *'I would ring PayPal to make sure it is from them'.*

The students did do the right thing to call PayPal directly to ask about the legitimacy of the email they have received. However, there is one issue with this method. Students are relying on the caller's knowledge of phishing emails in the PayPal customer service call centre to decide whether they reply to the email or not. The caller could believe in the legitimacy of the PayPal phishing email when described the email or if the individual sends the PayPal phishing email to the customer service advisor in PayPal. Also it is highly unlikely that the PayPal customer service representative will not know if the email is legitimate or not.

Student (37) suggested steps they would have taken if they received the email from PayPal:

'Ignore the email and check online banking or ring up the bank and delete email'.

Student (81) explained what they would do if they received from PayPal:

'Click the address of the sender and then maybe log into PayPal from a browser to check'.

Student (81) would check the origin of the email address from the sender to see if it is a phishing email and then will call the bank to check for any fraudulent activity on their PayPal account. It illustrates that the students are following the correct procedure when they receive a phishing email from PayPal. They will check for fraudulent activity on their online banking accounts or contact the bank directly. Students said they login to their

PayPal account in a search engine. Students said they do this to check the legitimacy of the email they have received.

Only a small proportion of students mentioned being aware of unknown links:

Student (143): *'Keep an eye on who's sending them and not opening unknown links'*

Student (122): *'Be extra vigilant and use common sense. Block any emails addresses that you have previously received phishing from'*

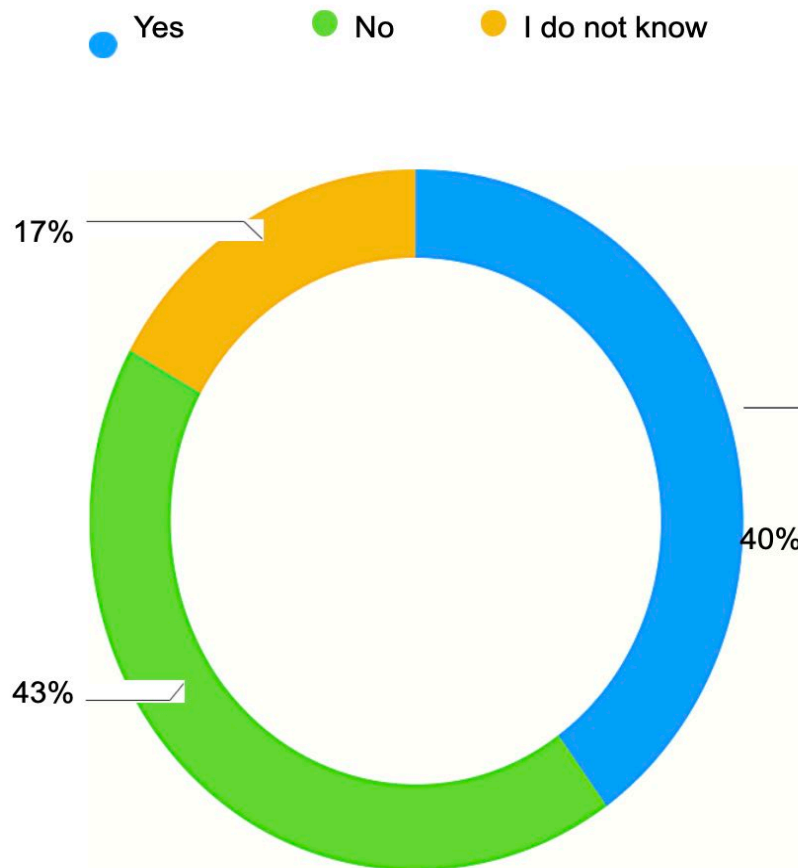
Student (170): *'Don't click links etc that don't seem real.'*

These students said they do not click on links, but they did not explain why they should not do that. They did not explain and identified further precautions needed against some types of phishing communication. It can make them prone to sophisticated phishing attacks in the future and failure to identify fraudulent aspects of phishing emails.

There were some responses about identifying some types of phishing variants which may contain grammatical and spelling mistakes. The participants mentioned about protection needed for devices as well as avoiding providing personal information:

Student (91): *'Looking for unusual names and email contacts and number. Any spelling mistakes on text. Have some protection on your devices. Don't give out personal information'*.

However, some users could be vulnerable to malware-based phishing if they download malware is malicious software installed on the victim's machine without their knowledge. Students mentioned having protection on their devices, but cybercriminals can trick a victim download malicious anti-virus software which contains malware or a virus. The fraudulent anti-virus software designed to destroy content on the system. Or the fake anti-virus software can steal private information from the user. The malware within the fraudulent anti-virus software is challenging to detect and remove because it can access confidential data and send it to the phisher (Emigh, 2006).



(Figure 5) Result of question 8 of questionnaire: *Do you use security safeguards (firewalls and/or VPN-Virtual Private Network) on your electronic devices that you may use on a daily basis in order to prevent you from receiving different types of phishing communication via email, phone or from text messages?*

The result of question 8 in (figure 5) emphasises that phishing variants will continue to be a cyber-security threat. The results revealed that only (71 students) 40% of students use security safeguards (firewalls/VPN) on their electronic devices. Some of the reasons provided by those who use security software on their electronic devices was:

Student 147: 'To safeguard against criminal entities.'

Student 153: 'I always use firewalls on my laptop to avoid being hacked and because most importantly I want my information to stay safe and protected.'

Student 69: 'I use a VPN on my phone and tablets and there is a firewall on my laptop.'

Student 71: 'Because I don't want my computer to be hacked'.

Student 168: 'To protect from malware or other corrupting/spyware and viruses.'

These responses illustrate that most students want their personal information to be encrypted and protected from malicious hacking attacks. Security software may prevent a small proportion of phishing-attacks. Security software does not defend against some types of phishing variants such as spear-phishing emails, SMS phishing, phishing emails links that may contain ransomware malware protected by most firewalls. VPNs are vulnerable to phishing attacks (Raphaely, 2020). The study wanted to identify students who use VPN to protect themselves from cyber-attacks and having security in their electronic devices (Sokolov et al., 2021).

43% (76 students) out of 177 students in the anonymised questionnaires do not use any security tools to protect their laptops, computers, mobile phones and tablets. It can pose a higher risk for them exposed to different social engineering attacks and advanced persistent threat spear-phishing attacks against their electronic devices designed to steal personal information to commit fraud. The questionnaire results found why the students did not have security software installed on their devices is they do not know how to install the software or do not know enough about a particular software needed to protect their devices.

They all given similar answers such as:

Student 79: 'I wouldn't know how to set it up'.

Student 18: 'Don't know how to get them'.

Student 113: 'I don't know how to use it'.

Student 62: 'Don't need to or know how'.

Student 13: 'Don't know what it is/does.'

Student 119: 'Do not know enough about them'.

The answers may have indicated a lack of understanding of what a security software does and familiarity with defence against some phishing attacks. They do not know how to install security software on their electronic devices. It demonstrates the lack of knowledge and awareness of different security software from users needed for protection against social engineering attacks (Abawajy and Kim 2010). The majority of online security threats based on the lack of user awareness of security software available for users to protect themselves against sophisticated cyber-attacks.

Students in the questionnaire who do not have security tools on their electronic devices may have weak knowledge and awareness about phishing threats. Some students may not know how to install software like anti-phishing filters and firewalls and knowledge about security precautions. A reason for the lack of understanding and awareness against phishing, spyware, trojans and worms may be the failure of students to keep themselves up to date with the latest security threats and security countermeasures that need to be installed on electronic devices to protect themselves against various cyber-attacks (Williams et al. 2020). It suggests that the participants may be vulnerable to new phishing attacks they may not be aware of in the future.

Factors that may contribute to some students not updating themselves about security tools to protect themselves against various social engineering attacks based on security awareness campaigns are mostly PowerPoint slides or digital posters on the university website and their workplace. These strategies are often ineffective and do not capture the attention of the students. Participants need to be aware of anything that requires them to open an attachment or click on a link. The perceived credibility of a message has an impact on persuasion (Petty and Cacioppo, 1986). It may have been an influential factor when students receive phishing variants. Evidence suggests that the appearance and the background credentials of phishing emails have a persuasive impact. The credibility of phishing communication includes message formation and layout. The visual appearance of a phishing email is well-written, well-organised and well-produced. It can increase the credibility and persuasion of a phishing email (Rao and Upadhyaya, 2009).

Raising awareness about phishing variants is not simple. It can be challenging to make people aware of phishing communication. People may not be thinking about phishing training when they get a phishing email (Williams et al., 2019). On the other hand, there are preventive measures that can protect users from malicious phishing websites. If a link cannot direct the user to open a malicious website, then the phishing attack cannot continue. A majority of up-to-date browsers may block phishing domains, websites and malware sites on desktop computers, laptops or tablets but do not always block malicious phishing communication on mobile devices. Phishing detection methods can include content-based approaches that examine phishing page content with URL features (Zhang et al., 2007).

The results of a focus group and the anonymised questionnaires suggested that part of the issue with not having security software's for electronic devices is due to a lack of awareness of the severity of phishing attacks. A lack of education on the benefits of using different security software protects from some phishing attacks.

Some policing and criminology students stated that they did not install security software on their electronic devices due to lack of affordability and refusing to purchase security software. Some responses provided were:

Student 113: *'I think you have to pay for these services. So, I don't because I am too poor and confusion.'*

Student 103: *'Don't want to pay for them.'*

Student 1: *'Can't afford it'.*

Some students may not have security software on their electronic devices because they may not be aware of free security software. Free security software can protect their personal information. Orhan and Karyda (2017) found that data breaches from phishing attacks stems from poor security practices and the human factor of being vulnerable to specific phishing variants.

The phishing email from the bank scenario was about fraudulent activity on their bank card. As a result, their bank deactivated their bank card temporarily. The majority of students said they call their bank or visit their local bank branch. The results showed that a majority of students might not fall for this type of phishing attack.

Some of the responses to the question were:

Student (88): *'I would go into a branch and check my account there or call the customer service phone number of the bank'.*

Student 89: *'Ring the bank or go in store straight away, and not reply to the email. Also, double check my card has been blocked/frozen'.*

Student 90: *'Ring the bank or go into branch.'*

Student 91: *'My bank doesn't email-they only call so I know it's phishing'.*

These students may have identified the email as a phishing email because their bank calls them, or they will call the bank or go into their branch if there has been fraudulent activity on their bank card. The result of the question indicated that the majority of the students might not be defrauded from a bank phishing email scenario in the anonymised questionnaire.

The result from question nine of the phishing email bank scenario indicated that the participants might have been aware of phishing emails from banks. Different factors can contribute to university student's awareness of bank phishing email who participated in the questionnaire. They may have previous security awareness training in their workplace or education setting about phishing emails from a bank. Some students may have general cybersecurity awareness about social engineering threats. Students could be aware of bank phishing emails by getting an email from their bank about phishing emails. Employees in the bank trained about phishing emails could have told the students about bank phishing emails by sending them emails or talking to them in the bank branch about different phishing communication.

Vishing Fraud discussion in focus group

There was a discussion about vishing using open-ended questioning to gauge as much information from the students understanding and awareness about vishing.

Student (5) said that:

Student 5: 'Often when you receive a phone call, they make out that like they know something. And if you are trying to identify details or get clarification, they will just continue to repeat the same question. You'll find that they know perhaps they don't know absolutely bugger all about you, besides your name, and going to try and get information from you and say, this happened, and they won't be able to tell you when or anything so what you should do when you answer these calls is not give, not being forthcoming with information and make sure they actually know things about you. Because otherwise all they've done is pull basic details of you from anywhere which is obviously public, and they are using that to try and deceive you'.

Student (5) identified the purpose of a vishing attack from a fraudster who is attempting to defraud them. A student explained a vishing phone call and did not share their personal information.

Student (4) mentioned one type of vishing variant which was a pre-recorded message:

'Some of them are pre-recorded aren't they and when you answer they carry on the conversation. And it is just a pre-recorded person.'

A student identified a vishing phone call but did not explain why they should not carry on the conversation. The student was prompted and asked for clarification but did not say why they should not carry on the conversation.

Student (2):

'If you reply...hello, they actually record the hello, and they can use it to get into your bank account... Like, they do require you to say hello into the phones activate the banking voice ID, which is what they're trying to phish for', This participant has identified a vishing variant which is attempting to phish for a particular word to access a victim's bank account. However, the participant did not know that answering an unknown number can alert vishing fraudsters that the number is active, which can lead to more calls in the future.

Student (3):

'This is like, if it's an unknown, or an unknown caller just don't answer it' which may result in less phone calls from fraudsters and a lower chance of being defrauded.

Student (1):

'My android phone doesn't come up with an unknown caller, if I am applying for jobs, and it comes with an ID that I don't know 9 times out of 10 I'm gonna answer it in case I want a job I don't know what the phone call is I am going to answer it'.

Student (1) could be defrauded because the student could provide their personal information if they receive a vishing phone call. But the student does have a point that if the student is waiting from a job offer the student will be likely answer the call from their phone. There is no solution to this issue to date because it is sometimes difficult for people to tell when they are being vished (Kaspersky, 2021).

The focus group students were asked about spear-phishing emails and the majority of students may not have known what it was.

Phishing communication from fraudsters

The focus group data found that by focusing on a particular subject. It identified some phishing variants that are difficult to avoid due to their sophistication (Wilkinson, 2004). A reason for focusing on some phishing communication is it may help the students to focus on one type of phishing. It can help them to discuss a phishing variant instead of different types of phishing in their response. It enabled me to gain a detailed understanding of one specific phishing attack used by a fraudster. Also, it showed when asked about potential security measures taken against phishing variants.

Student (5) stated that all emails should be checked by IT technicians before being sent to a user:

'All the emails are checked by the IT technicians before actually being received by the user. So, they'll check it to begin with see if this is an actual work email and then send to the actual person...whereas my personal point, is there's no filter it just goes straight to your inbox'.

It is problematic when several emails received by IT technicians throughout a day to check if it is a phishing email or not. It is not a possible solution to prevent different phishing communication because there are numerous emails sent to Canterbury Christ Church University every day. There is anti-filtering or anti-phishing software used to read all of these emails to check if they are malicious or not based on the rules that it uses. Also, some IT technicians may not identify some sophisticated phishing email due to which can still result in a phishing email sent to a user.

Student (1) stated that IT technicians are unable to notice some types of phishing variants: 'Sometimes you really can't tell though, because people SMS spoof and they do email header spoofing, they like to spoof the headers and said look, if you're an IT technician you see an email come through from your colleague, they'll just forward it through like it won't get caught by the filters automatically but if you do check the headers normally you can see it's been manipulated'

The student has given an example of a phishing email using 'email header spoofing' is when a header of an email may appear to be from a trustworthy source when sent to IT technicians.

Moreover, student (3) said that security measures against phishing variants is user awareness and specific protocols to deal with different phishing communication:

'Having specific protocols in place. Companies can deal with unknown callers, or out of hours callers or emails that don't look quite right. But it is also the user being aware of something that sounds too good to be true, it is, and if you don't know where it is from don't open it and if you are not expecting it don't open it. That sort of stuff'.

The student did not state that how a user could identify a phishing email. The student response was vague in some places: 'specific protocols in place to deal with unknown callers.' The student did not explain how it could be a potential social engineering risk to companies or how specific protocols can prevent some types of phishing attacks. It was followed up in the focus group by asking the students further questions. A student in the focus group stated that the preventive security measure against phishing variants was not to open it and but the respondent did not mention specific security measures or precautions to take against from some types of phishing attacks.

Student (2) did attempt to explain what spear-phishing was, and their answer lacked clarity:

'Isn't it just like spear-phishing is where they like targeting you as an individual, so I better be very like so say you work for an organisation. It's like, actually. So, instead of just sending it out to like many people would be like spear-phishing an exact company. And like trying to like to target the company on its own like create a, almost like a plan around it'.

The student did mention how a spear-phishing attack targets a specific organisation. But the student did not explain how spear-phishing works and how spear-phishing can defraud an organisation. It was evident that there was a lack of awareness about spear-phishing emails in the focus group. Computing students did not provide information about spear-phishing emails when asked further questions for clarification.

Students were asked about what smishing text message attacks are and if any of them received one in the past. The purpose of asking this question to the focus group is to gauge the research volunteers understanding, awareness and knowledge on smishing text message attacks.

Student (1) who was familiar with a smishing text message:

'There was one from student finance text message. It said there was a problem with their student finance, and they needed to update their bank details. And there was a link that you clicked on and soon as you clicked on it... sent you to the website'

Student (1) provided an example of a smishing text message from Student Finance England; but did not develop their answer by explaining why a user should not click on a link within a smishing text message. The student was encouraged to develop their answer by asking further questions in the focus group, but the student did not elaborate on the cyber-risks of clicking on the link in a smishing text message.

Students were asked further questions about how they would identify a smishing text message from fraudsters and a student provided an example:

'It will be like urgent your bank account will be deactivated in 24 hours. Click on this link kind of thing' the participant given an example of a smishing text message from a bank, but the participant did not explain the fraudulent aspects of a smishing text message and how a user can avoid being a victim of a smishing text message.'

This is related to studies in past that a message can overwhelm people and can result in fear which includes response time pressures with words described by a student: 'deactivated in 24 hours'. People may react increase their information processing under time pressure, and they are less likely to have confidence in their decision (Verplanken, 1993). In addition, a smishing text message may not state 'Click on this link...' but cybercriminals may make a smishing text message content persuasive by using a combination of appeals and structure. This is similar to a phishing emails whereby persuasive elements encourage recipients to accept them as genuine (Kim and Kim 2013).

Student (3) stated that: *'So wouldn't you just go to the site. Why would you click a link in a text? If my bank went to me your bank is shutting five hours you gotta sort it out. I am not going to text you... I'll go to the bank's website'*

This demonstrates the student's may be aware of a smishing text message the person will not send a text back but will navigate to the bank's official website directly.

Student (2) supported what the other student said: *'If someone says in a bank email, I need your login by clicking on this link, then that's dodgy.'*

Student (2) could be aware that the link in the smishing text message was from a fraudulent source but did not explain the identifying features of a smishing text message. The students in the focus group were aware of two types of smishing text messages from a bank and Student Finance England. However, there were not any specific responses in relation to the cyber-security risks of clicking on a link in smishing text messages. Additionally, the students did not discuss about the techniques used to detect smishing such as content-based filtering which involves examining the text in the SMS. Content-based filtering is based on the contents in a text message, smishing message is categorised. Students in the focus group did not discuss the features of a smishing text message and the different anti-smishing software they could use to reduce the probability of receiving a smishing text message.

Diksha and Ankit, (2017) suggested a smishing classifier to be used against smishing messages. A smishing classifier used a blacklist method, URL inspection method and content-based approaches to identify smishing messages. They used the URL inspection method to analyse the malicious processes of the URL and used the blacklist method to check if the URL is included in the blacklist. The students in the focus group were not aware of anti-smishing software which can increase the chance of them being defrauded by smishing text messages because they are not using anti-smishing software. In contrast the issue with content-based filtering is it can be expensive and can cause the privacy of the user to be invaded (Xu and Xiang et al., 2012).

Students were asked a question in relation to a fictional scenario which was in fact a smishing text message. The scenario was about if they were expecting a delivery during the Christmas period and they had received a text message which had their delivery details such as their order number and so on would they click on a link in the text message. Students' awareness levels of about the fictional scenario smishing text message was varied.

Student (4) who was aware of one type of smishing text message variant said:

'It could have been a database breach, and someone could have gone through and like coordinate like a spear phishing attack and actually like what made it so they wrote a script which just fills in the gaps... which is reasons why you just don't click links on emails or text'

The student classified a smishing text message could be sent to a person to look like a spear-phishing attack. But the student did not describe specific features of a smishing text message sent by a fraudster or why a person should not click on links on a smishing text message if it appears to be fraudulent.

In comparison another student (2) said that:

'Wouldn't most courier places come up with a text message saying it is from Amazon or DPD on your phone... if they somehow did that you will believe it is them so...'

The student could fall for a smishing text message. The student assumed that if the text message appeared to be from Amazon or DPD could be legitimate. The student may think that the text message is trustworthy if a cybercriminal crafted a sophisticated smishing text message originating from a courier company such as Amazon or DPD.

Scenario-based discussion asked about PDF document attachment from a University Lecturer

Computing students were asked in a focus group to answer a question from a fictional scenario about a phishing email that includes legitimate details so that they will download a PDF file sent by their lecturer or someone they know. Computing students all said that they download a PDF file from the scenario-based phishing email.

Student (4) in response to the question that a file was downloaded it will be scanned from their computer and will give a warning about the PDF file in an email. This is true for most anti-virus software that scan email downloads before they are opened. Also, webmail will scan the email at the server. However, it is possible for new malware variants that are unknown by the anti-virus software to get through. Viruses and malware change rapidly and therefore 100% protection is not possible from anti-virus tools and anti-virus software

(Keepnet Labs, 2020). For example, trojan viruses and network worms actively search for antivirus programs from a victim computer and the malware will attempt to block the antivirus software, damage the antivirus databases and prevent the antivirus software's update processes (Kaspersky 2021) :

'But most security software now scan anything from an email... like my one anything I download like a PDF it will give you a warning so. My computer isn't a problem like my phone might be'.

The student may not know that if you download a PDF document to their computer or mobile phone. It will download a malicious file to gain access to their computer or mobile phone. The attached file could be a malicious PDF attachment. Once opened by the respondent, will execute a script to infiltrate the person's system. Cybercriminals may choose to take remote control over their system Remote Access Trojan (RAT). Steal their credentials (keyloggers), download spyware to monitor the network, gather as well as extract files or encrypt the person's files on their computer and demand a ransom payment (ransomware), or increase their privileges on the victim's computer (Europol, 2019).

A student added that malware signature used in malicious PDF files in phishing emails can evade some email filters once downloaded:

'Depends on the signature of the malware a lot of PDFs if you open a PDF, it could be like, but especially with Adobe. It might not scan the malware signature, but it might have some sort of like evasion software on it'.

It could depend on the malware variants such as Adware, Crimeware, Rootkits and Spyware. Malware can develop rapidly and become complicated and evolve into more sophisticated attacks. Phishing emails with malware can carry out executable code to the host and replicate it. Some malware in phishing emails embeds compromised documents and hide a malicious file type like a PDF file (Islam and Ozkaya 2019).

The findings of the focus group were surprising. Because there was an assumption on my behalf as a researcher that the computing students knew the threat of malicious email attachments pose to them if they do not do thorough checks once they receive an email from a known or unknown recipient. A malicious attachment could contain dangerous attachments that can trigger keyloggers, ransomware, and other malware variants once opened by a victim (Ivanov et al., 2021). Anti-virus software cannot do thorough checks of phishing email communication all the time. For example, spear-phishing attacks and

malware variants in phishing communication can bypass anti-virus technologies. It can take hours for anti-virus technology vectors to investigate new attacks and deploy updates or patches (Keepnet Labs, 2020).

Prevention of Phishing Attacks suggestions from computing students

Prevention of phishing attacks is if the university can promote or prevent people from being defrauded by different phishing attacks. Student 3 suggested to:

'Put up bulletins... But then again, like someone could use that as like a technique, if the uni is putting up bulletins they could put up a fake bulletin. But it's just, you can't really catch it, it's all user error like you need to sort of like train yourself to detect when there's like maybe like grammatical errors and like the spacing is wrong. Or like the link looks sketchy... because on Outlook, you can do redirects and like you need to have a look at that where it's redirecting to'.

Student (3) suggested that university announcements against specific phishing variants can be helpful. However, cyber-criminals can exploit this by uploading fake bulletins. A student concluded that it is mainly user-error. If there are university bulletins about phishing attacks, some students will still click on links or download files from different phishing communication. The student added that a phishing variant detected from grammatical errors or the spacing could be wrong. These are for some types of phishing variants but not all of them.

On the other hand, more phishing variants are becoming sophisticated and thus do not have grammatical or spacing errors. Moreover, a student said the user needs to look at where the link is redirecting the user. It can be problematic because the malicious link could contain a malware variant that can be executed and downloaded to the recipient's system in a phishing email (Tierney, 2018). Or the link and the content of a phishing email may persuade a user to click on the link. The majority of phishing emails may include company domain names or logos to increase credibility and convince recipients. People are more likely to be motivated to accept the messages if the phishing emails use rational and emotional appeals. People may believe that the content of an email is relevant to them. Thus, they are more likely to respond to a phishing email (Kim and Kim, 2013).

Some users may unintentionally download plug-ins from third-party providers. It can lead to more vulnerabilities in the internet browser (Chiew, Yong and Tan, 2018). This type of phishing attack is difficult to detect and prevent even if the computer system is updated. An additional limitation of user training is not possible to educate all users about different security tools. Users may be confused with the range of security tools against phishing variants. If some users decide not to use security tools, they will be vulnerable to phishing attacks.

Previous studies on user training have shown improvements in phishing detection, but most studies have not tested their user training against phishing variants for a specific time. Studies on phishing training are based on scenarios and are about different phishing communication. It will be interesting if the participants are not informed about the test and observe users on how they will respond to phishing emails and their variants. Findings in most studies show that education is beneficial and is needed. But it is not a solution to phishing. Also, false positives can deter users from using security tools if they block users' emails regularly or block them from visiting websites that are not phishing websites or associated with phishing domains (Purkait, 2012). Some of the challenges of education and training programs is ensuring that the research participants remember the information they have learned after the information provided from the user training about different types of phishing communication (Summer and Yuan, 2019).

A student discussed blacklisting certain phishing domains can be used as a preventative security measure against some types of phishing variants:

'You could domains. Certain providers do blacklist certain domains if they know they are phishing domains.'

However, a problem with crawling and blacklisting phishing domains could be that the anti-phishing organisations will find themselves combating different phishing attacks from online fraudsters daily. Plug-in browsers could detect phishing attacks based on blacklisted phishing domains, but they do not resolve the zero-day phishing attack (Ross and Jackson et al., 2005). A web crawler or an internet bot can send automated scripts to browse webpages to find threats from phishing variants such as zero-day phishing. However, this may be ineffective against new phishing attacks with malware capable of bypassing web crawler tools.

A malformed URL prefix attack in phishing emails use tactics such as displaying fraudulent display names to trick users into thinking the email is internal. The phishing emails use unknown domains and senders to bypass filters that look for known malicious senders. Payloads within the links use open redirector domains. Phishing emails urged users to make a mistake. The phishing emails use prefixes to include a second forward slash in favour of a backslash. For example, http:// and then add a malicious URL into the prefix before and adds a legitimate domain name treated as subdirectories of a malicious page. It makes it possible to create a phishing website (Vigliarolo, 2021).

Additionally, blacklisting approaches are only useful if they are maintained and updated regularly. A disadvantage of blacklisting different phishing domain are new phishing sites that are not blacklisted. New phishing websites could not be in the database from the blacklisting software that can avoid filters (Hämmerli and Sommer, 2007). The majority of phishing sites that are blacklisted are temporary and exist for less than 20 hours. Phishing sites change URLs regularly is known as fast flux (Moore and Clayton, 2007). The URL blacklisting approach fails to identify some phishing variants. The blacklisting approach fails to detect spear-phishing emails, especially when cyber-criminals' targets sites such as company intranets (Afroz and Greenstadt, 2009). Phishing websites can grow in sophistication and can bypass defences (Oest et al., 2020).

Protection against phishing attacks in focus group

Student (3) suggested in order to be protected against phishing attacks is:

'Or maybe having like filters that catches certain words or phrases. But then again, that could start filtering emails which are not phishing emails, and if there is a security issue and the admin is trying to get a password change.'

The use of filters that attempts to prevent phishing emails is using filters and content analysis. Techniques used to intercept phishing emails are Bayesian filters. Nevertheless, the effectiveness of filtering phishing emails is on regular filter training and the availability of anti-spam tools. Filtering software is not perfect, and some phishing emails may bypass filters and reach victims (Hämmerli and Sommer, 2007). A problematic feature of email filtering is a user may not choose to use the spam or phishing filter. Some users may

forget to update the filter periodically. It may result in them becoming a victim of phishing. Some issues with filters are it generates false positive. It can result in to trust the use of filters less. Filters can often flag emails as phishing email, which can create inconvenience for users. Users may not use the anti-phishing filters if it repetitively blocks or deletes emails as phishing emails. Email filtering may not be useful for phishing detection. Filters used to classify email content based on keywords may filter words that appear in emails that not classified as spam or phishing. Fraudsters find strategies regularly to make phishing emails appear legitimate to bypass filters. For example, in a spam filtering system, attackers add irreverent words to evade system detection (Zhang et al., 2021). Most students are probably using anti-spam or phishing filters without realising it. These are installed at a mail server level. This may be used for the students' university email servers.

Data collected from anonymised questionnaires and focus group suggested that students did know about some phishing variants. In the focus group with computing students, several students did not know what spear phishing was. A student did define spear-phishing email but did not explain the identifying features of a spear-phishing attack. The focus group found that the computing students provided recommendations for security software and preventive measures against phishing attacks, but their responses lacked clarity and shown their knowledge gap.

Students said they would compartmentalise their system and only open emails that they know. It was a vague response and did not indicate whether the participants can identify spear-phishing emails which can appear in their personal or university emails. Some participants went off-topic about the discussion suggesting security measures against different types of phishing communication. Some preventive security recommendations made about some phishing variants, but these may be ineffective. The result of a focus group found that awareness from some students about phishing variants was limited. There was not enough time within the focus group to reach this conclusion. It was due to the allocated time (30 minutes) put aside with the focus group computing students. The specific time in the focus group was due to various reasons. The focus group was 30 minutes because the students did not miss the majority of their lesson time. I did not want the focus group to take too long. A reason for it was they may become restless and may not provide useful feedback. The focus group found they were nervous at the beginning of the focus group. Some students did not answer and participate in group discussions in

the first 5 minutes of the focus group. It changed when the focus group progressed. The students began to participate and share their thoughts about different phishing communication.

They did discuss security measures such as filtering software to block some phishing emails, but they did not explain precautions they should take if a phishing email bypasses filtering software. There was a gap in knowledge from a student. It could lead to further cyberattacks on the university database or other critical infrastructure if it is not dealt with accordingly. Anti-phishing filters may occasionally provide misleading confirming indicators that a phishing website is legitimate (Abu-Nimeh, 2008). The anonymised questionnaires results may suggest that students who had security software on their electronic devices may be vulnerable to phishing attacks such as vishing, smishing, pharming and spear-phishing. Different types of sophisticated phishing communication can bypass firewalls and anti-phishing filters. They can perform malicious activities on a victim's device. Some students are not aware that they have received a phishing communication. The students are more likely to be defrauded by phishing variants. Phishing is a common and easy way for cybercriminals to bypass security measures (Symantec, 2016; Blog, 2016; Verizon, 2015). Phishing email variants are efficient because they exploit human psychology and make phishing communication appear trustworthy (Jagatic et.,2007).

Cybercriminals use sophisticated methods to send a phishing email that replaces links with malicious links that redirect a victim to a phishing webpage that may use real company logos (Mehan, 2016). The results from the anonymised questionnaires and focus group found that students did not mention how they should be cautious from sophisticated phishing email variants redirecting them to a phishing webpage. A student's perception of phishing susceptibility may not be on a phishing communication encounter. But it can be influenced by their existing beliefs of phishing. The user learns and updates their phishing susceptibility by incorporating the experience with a new phishing email variant. An issue of this learning experience is likely to be different among students. Thus they may be defrauded to new phishing email variants (Kim and Kim, 2013). Spear phishing emails are sophisticated in their design and approach compared to generic phishing emails, making them difficult to identify. The attack vectors from spear-phishing emails are perpetually evolving. Spear-phishing emails can be a cyber threat to students (Williams and Joinson, 2020).

Some students defrauded by phishing variants in anonymised questionnaires and a focus group. It is because of underlying factors. One reason is phishing detection and when a student completes the task intended by the fraudster. Some students defrauded by phishing emails: download a file by clicking on a link, downloading a picture that may contain viruses, trojans, spyware and worm and provide personal information or login information. It could happen when students cannot identify the inconsistencies of the email content. A student may not identify phishing cues in the phishing email. In some cases, a student may know an email is fraudulent but superseded by the perceived credibility of the content of a phishing email. Another factor that may lead to students' failure to identify phishing emails. They may not have the ability to verify some fraudulent phishing emails like a spear-phishing email (Wang et al., 2009).

Other factors of students falling for phishing attacks could be from Canterbury Christ University policies. It does not include how students and staff can identify different types of phishing emails and how students and staff can report phishing emails to IT staff and from their university email. There are several reasons that the university policies might not provide enough information and advice about threats from phishing attacks. The policy zone section is not easy to find on the website. The user has to navigate to the bottom of the website. The policies on guidance on IT regulations and the email policy are generalised and does not include any information about different types of phishing variants. The email policy (2013) is outdated and does not explicitly include information about phishing emails and the preventive measures that can be taken against phishing emails.

The university website does not have a section where students can report malicious phishing emails to IT staff members. Additionally, the university policy is not clear about how the students can report a phishing email and their variants to the university. Students have to agree to the 'Fair Use Policies' when they get a new university account. The policies must be accepted when students log in to a computer. An issue with most policy documents and terms and conditions is that some students deliberately skip them when they sign in to a university computer and accept them without ever reading them.

On the other hand, there is an 'phishing button' in the students' Microsoft Outlook University student email account whereby students can report incidents of suspected phishing emails, but this may not be noticeable by some students because the phishing button is not easy to find if students have installed the university mail client app on their personal computers or if they are using the mail client on a webpage online.

Conclusion

The study found a range of factors in which students might fall victim to different types of phishing attacks. Results from the focus group identified that the majority of students with exception of one student did not know what spear-phishing was. In the focus group the students failed to recognise spear-phishing emails. Similarly, a spear-phishing scenario question was asked in the questionnaire and found that most students fall victim to the spear-phishing attack. Awareness about spear phishing emails from the focus group and the questionnaires could be because of different reasons such as lack of knowledge and awareness about spear phishing emails, the layout, cues that may be used and the appearance of the email can make it difficult for some users to detect spear phishing emails. Some students are not be able to identify the fraudulent features of spear phishing emails.

Additionally, when students were asked about smishing text messages a small portion of participants mentioned anti-smishing software which can be used against smishing attacks. Anonymised data collected from the focus group and questionnaires illustrated that the majority of participants either did not know or mentioned about the features of a smishing text message. Some students might be a victim to a smishing attack based on the results in the anonymised questionnaire because they said they would have either opened the link in the text message or pay for the delivery cost of an item they would have been expecting to be delivered to them.

User education and training about social engineering attacks from different types of phishing attacks can be used to explain the need of taking security measures but changing the users' knowledge and understanding does not mean that they will change their behaviour. The majority of organisations provide security instructions to users and they expect these instructions to be followed. This can be problematic as some users may have a set of beliefs and attitudes who do not comply with security policies (Weirich and Sasse, 2001). The statistical information collected from the questionnaires and the focus group

could illustrate that some users do not believe that they are personally at risk against phishing attacks. They could think that they will be not held accountable if they do not follow security regulations or use anti-phishing to protect themselves from some types of phishing variants (Cranor and Garfinkel, 2005). A study carried out by Furnell (2007) about users being able to identify phishing is similar to this study when participants are asked about different types of phishing communication. The results from the questionnaires and the focus group found that the majority of the students might be lacking the basic level of security and general awareness against some types phishing variants.

Some of the limitations of phishing-related educational and awareness training shown limited success in terms of reducing susceptibility to different types of phishing (Williams and Joinson 2020). NCSC guidance in relation to the challenges and limitations of anti-phishing education by overwhelming users in a complex threat landscape from social-engineering attacks (NCSC, 2018), it is necessary to use a mixture of technical defences with user awareness and education about phishing attacks which are used regularly by fraudsters and how to report them is highlighted (NCSC, 2016). There may be a lack of evidence user training about different phishing communication can reduce the phishing threat and the extent in which students are likely to engage with the awareness and education interventions. Thus, it is fundamental to consider if students currently view phishing-related information, and if they engage with the content and various factors that may influence this (Williams and Joinson 2020).

The perception of different types of phishing emails from students differed. The statistical information collected from the focus group and questionnaires found that there was a split between respondents who are aware of some types of phishing variants but are unable to provide further insight into how they can be identified and security software that can be used against different types of phishing. Other participants who did not have knowledge about anti-phishing software are more likely to be victims of phishing emails. This was reflected in the questionnaire results whereby the participants simply downloaded an email attachment to their electronic devices. Nonetheless, some participants who said that they have security software on their electronic devices, and they stated that they have technical knowledge about phishing emails did say that they would download email attachments from people that they know. The reason for this might be that they may not be aware of the cybersecurity risks of downloading unknown attachments which may

appear to be from someone they know. Also, it can be due to effectiveness of phishing because of the cognitive nature of phishing variants to encourage students to download attachments on their electronic devices. A phishing email manipulates a user's perception and relies on the user's changed actions to carry out further attacks (Cybenko et al., 2002).

Perception of phishing variants is explored in the study which reviewed factors that may influence students engage with information presented to them in a phishing variant. It might be possible that a lack of engagement with information sources about phishing variants might have contributed to their limited effectiveness (Williams and Joinson 2020). The data sample from the focus group and anonymised questionnaires investigated who may be defrauded by fraudsters from different phishing variants which hide malicious content and send phishing communication to appear to be from a trustworthy source and may have had resulted in students who may not identify it as a phishing variant. The susceptibility of students to some phishing variants is when they have difficulties detecting fraudulent communication from cybercriminals. Some students were unaware of the threat from phishing variants and thus they are more likely to have their personal information to be targeted by fraudsters and they may lack the perspective needed to identify threats from phishing attacks and may not take precautions such as using security tools when carrying out online activities.

Recommendations are on the anonymised data collected from the anonymised questionnaires and the focus group. The email to the head of IT includes a summary of the results and findings of the study. An email sent can find solutions for phishing communications attacks when the current research has finished. The head of IT in Canterbury Christ Church University can review and may change or adapt the existing phishing policy in the university. One positive impact of the study is it may lead to policy change in the university which can reduce the possibility of students being victimised from phishing attacks in the future. Also, the existing phishing policy if updated or adapted from the head of IT in Canterbury Christ Church University might make the university more resistant against sophisticated phishing attacks. Another recommendation from the current study could be anti-phishing software installed on university computers to filter and block some phishing attacks. An additional recommendation to the current research is to organise online training sessions at Canterbury Christ Church University. Online training sessions will have people who specialise or are experts in social engineering attacks to

discuss the dangers of phishing attacks and preventive measures against phishing variants to avoid students being a victim of phishing communication in the university.

Another positive impact this research has made is it found a gap in knowledge from specific phishing attacks. A possible solution is online training sessions with students to be aware of new phishing attacks deployed by hackers. It can be done online due to the COVID-19 pandemic and encourage students to complete training programmes about phishing attacks online. The training will be optional for students who may wish to take the training courses in their university courses induction programmes. In the current study's recommendations section, Caldwell's (2013) study is used as a recommendation to introduce student training sessions about phishing attacks they may receive in their student emails or personal emails that may further cyberattack without their knowledge. To address a gap in awareness about different phishing attacks, students can have training sessions at university. It can be beneficial for students because phishing emails and their variants are evolving continuously from cybercriminals.

I have learnt that there were some gaps in knowledge from some students within the data collection sample. Some phishing attacks that users are not aware of sent from hackers and could be problematic for the university. However, students can know about the cyber-threats of phishing attacks by informing the university IT team that can organise workshops with students to be aware of different types of phishing attacks.

I have learnt that security countermeasures against phishing attacks may not be enough to prevent students from being victims of phishing fraud. It requires the recipient of a phishing communication to carefully read and analyse the fraudulent communication so the victim could avoid phishing attack variants. Additionally, due to the surge of new zero-day phishing attacks, it is sometimes difficult to avoid being a victim of phishing fraud. Online fraudsters are using new methods to steal personal information and to launch further cyber-attacks against unsuspecting victims. For example, some cybercriminals use malicious tools that use AI (Artificial intelligence) to launch phishing attacks (Yamin et al., 2021). I have learnt that there is a gap in knowledge for some specific types of phishing attacks towards victims; it can be problematic because it may lead to further cyber-attacks towards other targeted servers or databases from cybercriminals.

The study collated a specific sample size of students who are studying policing, criminology and computing. This enabled the analysis of the research to focus on their perception and awareness of phishing attack variants. The advantage of focusing upon a specific student population was it enabled me to gain a focused insight and understanding into the gap in knowledge from the students when they were questioned about different types of phishing attacks. These outputs can be developed further in future studies and used by law enforcement agencies in the future to mitigate and reduce the threat of phishing at a larger scale.

Limitations and Further Studies

The study focused on a specific population of students from the School of Law, Policing and Social Sciences and computing students. This limitation is a result of the use of anonymised questionnaires and a focus group as a data collection approach on a small portion of the student population from Canterbury Christ Church University which could have looked at different departments in the university to find out their awareness and perception of different phishing variants. The results collected in the current research did not provide full evidence for the awareness levels and perception of phishing variants from universities nationwide in the UK. Future studies could look at universities nationwide in the UK to find out students' awareness and perception of phishing variants to validate the current findings. Other studies can be sponsored by the UK government which can conduct research on a wider scale from online users and their awareness and perception of different phishing attacks in different locations in the UK. However, to indirectly address this issue, the study focused on a specific number of university students to generate detailed analysis of the results from a focus group and anonymised questionnaires in order to find out the underlying factors in which students fall victim to different types of phishing attacks as well as the reviewing what governments and police agencies worldwide do to investigate and mitigate phishing attacks.

Unfortunately, due to the lack of resources, time and funding I am unable to make comparison between students in different countries on their awareness levels of phishing attacks. However, this can be done by law enforcement government research funded agencies who work for Europol, Interpol and the NCA. Moreover, the research might be proven to be useful for banking cyber-defence and digital forensics sectors who analyse and might deal with malware variants from phishing attacks. Thus, the awareness of phishing fraud is essential to banking staff as well as digital forensics experts who need victims to be aware of certain phishing attacks. This may not always be preventable due to zero-day phishing attacks and sophisticated malware variants which has not been detected by firewalls or digital forensics employees themselves.

Future studies may explore data from annual financial cost of phishing globally and correspond to the number of victims who had been defrauded by phishing variants. Similarly, new studies are needed to address limited information about the impact of different phishing attacks on students studying at universities abroad compared to universities in the UK and if they reported phishing attacks. Reporting of phishing variants to international police forces and government agencies around the world investigating different phishing attacks can be evaluated and the process itself could be reviewed to see if it is effective to reduce the number of victims from phishing variants and as a result future studies could review the money saved from reducing the number of victims being defrauded by different phishing communication by cybercriminals.

Another future study which was not explored in the study could be about cyber risk from Dark Web marketplaces that may lead to different types phishing attacks from cybercriminals and the role of international police forces and governments that may carry out surveillance or take down some illegal financial services which are operated on the Dark Web.

Other future studies could evaluate the impact of the COVID-19 pandemic on the wider student population in universities and the rise in phishing attacks that use coronavirus themed subjects and content within phishing variants which are designed by cybercriminals for malicious purposes. Future studies could look at international threat actors behind global COVID-19 phishing campaigns which use different tactics to evade detection by using sophisticated email templates and attachments such as a compressed file as a link (LNK file) or .rtf file extension directs to a powershell.exe with obfuscated data as parameters (Thaware, 2020). The malicious attachments could be forensically examined which may use URL obfuscation using PowerShell script. Mitigation and defence strategies against COVID-19 phishing variants could be recommenced in the studies. Furthermore, it may be useful to share intelligence and work collaboratively with law enforcement agencies, private companies and public cyber defence companies which may specialise in tracing phishing attacks from organised international criminal syndicates, individuals, or hacker groups. However, this may be proven to be problematic if some countries have different rules on their cyber law enforcement laws.

On the other hand, cooperation leads to arrests and according to Interpol's Financial Crime unit (2020) stated the importance of a coordinated response to phishing this is taking into account: security countermeasures, inadequate anti-virus controls or anti-malware applications, key staff working with critical infrastructure and network vulnerabilities which may breach a database further if stronger countermeasures is not put in place once a victim clicks on a link or falls victim to a specific phishing attack. Thus, future studies could look at the underlying factors from students on a wider scale within universities. However, according to Europol's IOCTA publication (2020) phishing has become challenging to detect because the majority of phishing emails and phishing sites are almost identical to the real ones. Also, phishing campaigns created by cybercriminals are automated and produced at a faster rate which may force respondents to act quicker than before and in some cases it takes one day which can lead to a credential leak from a specific phishing attack.

A future study from the current study is another data collection method which may come into use is structured interview with victims of phishing and how they received support from the police and independent non-governmental organisations.

The study found a range of awareness levels from students about phishing attacks and what they consider as security countermeasures to avoid becoming a victim of phishing fraud. Also, the study can be proven to be effective because it can be used to explore a wider population of students and this may result in a deeper insight into why some students become victims to different types of phishing attacks. One of the positive impacts of this study is the College of Policing, UK Government researchers and some European universities or international universities can use this study and increase the sample size nationally and even internationally for example comparing the victims of phishing fraud in Germany universities and UK universities and analyse their awareness levels of different types of phishing communication from fraudsters.

Limitations of the study is the paper based questionnaire wording could be seen as misleading in terms of making students into thinking for example making an informed decision and response to a specific scenario based question is a spear phishing email or not from an online fraudster.

Bibliography

Aijaz NU., Misbahuddin M. and Raziuddin S. (2021). *Survey on DNS-Specific Security Issues and Solution Approaches*. In Data Science and Security. Lecture Notes in Networks and Systems, volume 132. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-15-5309-7_9

Arivukarasi, M. and Antonidoss, A. (2020). *DeepPhish: Automated Phishing Detection Using Recurrent Neural Network*. In: Suresh P., Saravanakumar U., Hussein Al Salameh M. (eds) *Advances in Smart System Technologies. Advances in Intelligent Systems and Computing*, vol 1163. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-15-5029-4_18

Almomani, A., Nawasrah, A.A, Alauthman, M., Betar, M.A.A and Meziane, F. (2021). *Botnet detection used fast-flux technique, based on adaptive dynamic evolving spiking neural network algorithm*. *International Journal of Ad Hoc and Ubiquitous Computing*, Volume 36, Issue 1, DOI: <https://doi.org/10.1504/IJAHUC.2021.112981>

Abraham, S. (2021). *Can PDF have Virus?* MalwareFox, available at: <https://www.malwarefox.com/can-pdf-have-virus/>

Ablon, L. (2018). *Data Thieves. The Motivations of Cyber Threat Actors and Their Use and Monetisation of Stolen Data*. Rand Corporation, Santa Monica, Calif. Available at: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Action Fraud (2020). *Coronavirus scam costs victims over £800k in one month*. Available at: <https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month>

Action Fraud (2020). *Coronavirus-related fraud reports increase by 400% in March*. Available at: <https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march>

Action Fraud (2020). *What is Action Fraud?* Available at: <https://www.actionfraud.police.uk/what-is-action-fraud>

Action Fraud (2020). *COVID-19 related scams - news and resources*. Available at:
<https://www.actionfraud.police.uk/covid19>

Aragues, A. (2017) *The challenge of attribution by IP address*. Available at:
[https:// www.itproportal.com/features/the-challenge-of-attribution-by-ip-address/](https://www.itproportal.com/features/the-challenge-of-attribution-by-ip-address/)

Axinn, W. and Pearce, L. (2006). *Mixed Method Data Collection Strategies New Perspectives on Anthropological and Social Demography*. New York: Cambridge University Press.

Arachchilage, N. A. G. , & Love, S. (2013). *A game design framework for avoiding phishing attacks*. Computers in Human Behaviour. Volume 29, Issue 3. DOI:
<https://doi.org/10.1016/j.chb.2012.12.018>

Arachchilage, N. A. G. , & Love, S. (2014). *Security awareness of computer users: A phishing threat avoidance perspective*. Computers in Human Behaviour , Volume 38. DOI:
<https://doi.org/10.1016/j.chb.2014.05.046>

APWG (2021). *Phishing Activity Trends Report*. Available at:
https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

Azeez A.N., Salaudeen, B.B., Misra, S., Damaševičius, R. and Maskeliūnas, R. (2020). *Identifying phishing attacks in communication networks using URL consistency features*. International Journal of Electronic Security and Digital Forensics. Volume 12, Issue 2, DOI: 10.1504/IJESDF.2020.106318

Abu-Nimeh, S. (2008). *Bypassing security toolbars and phishing filters via DNS poisoning*. IEEE GLOBECOM. Proceeding of the Global Telecommunications Conference. New Orleans, LO.

Abawajy, J. and Kim, TH. (2010). *Performance analysis of cyber security awareness delivery methods. Security technology, disaster recovery and business continuity. In: Communication in computer and information science*. Volume 122. Springer-Verlag.

AlEroud, A., Zhou, L. (2017). *Phishing environments, techniques, and countermeasures: a survey*. Computer Security.

Afroz, S. and Greenstadt, R. (2009). *PhishZoo: Detecting Phishing Websites By Looking at Them*. Drexel University, Philadelphia.

Aurini, J., Heath, M. and Howells, S. (2016). *The 'How To' Of Qualitative Research*. London: Sage.

Ayob, Z. and Weir G.R.S. (2021). *Cyber Physical, Computer and Automation System, Advances in Intelligent Systems and Computing*. Springer Nature, Singapore Pte Ltd. DOI: https://doi.org/10.1007/978-981-33-4062-6_3

Akinwale, A., Sodiya, S., Afolabi, O., Orunsolu, A., (2018). *A Users' Awareness Study and Influence of Socio-Demography Perception of Anti-Phishing Security Tips*. Volume 7, Issue 2, DOI: 10.18267/j.aip.119

Alsharnouby M., Alaca F., Chiasson S. (2015). *Why phishing still works: User strategies for combating phishing attacks*.

Athanassoulis, N., Wilson, J. (2009). *When is deception in research ethical?* Clinical Ethics, Volume 4, Issue 1

Ablon., L, Libicki., M. and Golay., A (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Rand Corporation. Available at: <https://books.google.co.uk/books?id=DodFAwAAQBAJ&printsec=frontcover&dq=online+carding+market+on+the+darknet&hl=en&sa=X&ved=0ahUKEwjmf3Kr4fgAhUUVBUIHXUTDUUQ6AEILTAB#v=onepage&q&f=false>

Action Fraud (2019). *SCAM WARNING - Fake Virgin Media emails*. Available at: [https:// www.actionfraudalert.co.uk/da/264052/SCAM%20WARNING%20-%20Fake%20Virgin%20Media%20emails.html](https://www.actionfraudalert.co.uk/da/264052/SCAM%20WARNING%20-%20Fake%20Virgin%20Media%20emails.html) [Accessed 13th March 2019].

Akhgar, B., Staniforth, A. and Bosco, F. (2014). *Cybercrime and cyber terrorism investigator's handbook*. Waltham, MA: Syngress.

Akila, S. (2018). *Cost-sensitive Risk Induced Bayesian Inference Bagging (RIBIB) for credit card fraud detection*. Journal of Computational Science, Volume: 27, DOI: [https:// doi.org/10.1016/j.jocs.2018.06.009](https://doi.org/10.1016/j.jocs.2018.06.009)

Abdelhamid, N., Ayesh, A. and Thabtah, F. (2014). *Phishing detection based associative classification data mining*.

Atkins, B., and W. Huang. (2013). *A Study of Social Engineering in Online Frauds*. Open Journal of Social Sciences, Volume 1, Issue 3, DOI:10.4236/jss.2013.13004

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Indianapolis, Indiana: John Wiley and Sons.

Align (2018). *Common Phishing Attack Vectors*. Available at: <https://www.align.com/blog/common-phishing-attack-vectors>

Armano ,G., Marchal S. and Asokan N (2016). *Real-time client-side phishing prevention add-on*. In: 2016 IEEE 36th international conference on distributed computing systems (ICDCS). DOI: <https://doi.org/10.1109/icdcs.2016.44>

Allodi, L., Chotza, T., Panina E. and Zannone, N. (2020). *The Need for New Antiphishing Measures Against Spear-Phishing Attacks*. IEEE Security and Privacy. Volume, 18, no. 2. DOI: 10.1109/MSEC.2019.2940952.

Barrios, M., Villarroja, A., Borrego, Á., and Ollé, C. (2011). *Response rates and data quality in web and mail surveys administered in PhD holders*. Social Science Computer Review. Volume 29, Issue 2

Bachman, R. and Schutt, R. (2013). *The Practice of Research in Criminology and Criminal Justice*. Los Angeles, Calif: Sage.

Bryant, A. (2011). *Leading issues in business research methods*. Reading: Academic Conferences Limited.

Bhandari, P. (2020). *An introduction to qualitative research*. Available at: <https://www.scribbr.com/methodology/qualitative-research/>

Brush, K. (2020). *Cybercrime*. TechTarget, SearchSecurity. Available at: <https://searchsecurity.techtarget.com/definition/cybercrime>

Bertrand, J. Brown, J. and Ward, V. (1992). *Techniques for Analysing Focus Group Data*. Evaluation Review, Volume 16.

Brannen, J. (2017). *Mixing Methods: Qualitative and Quantitative Research*. Abingdon, Oxon: Routledge.

Bryman, A. (2008). *Why Do Researchers Integrate/Combine/Mesh/Blend/Mix/Fuse Quantitative and Qualitative Research?* in M. Bergman (ed.), *Advances in Mixed Methods Research*. London: Sage

Bank of England (2020). *Privacy and the Bank of England*. Available at: <https://www.bankofengland.co.uk/legal/privacy>

Babbie, E.R. (2010). *The Practice of Social Research*. 12th edition. Belmont, CA: Wadsworth Cengage.

Bryman A. (n.d.). *Triangulation*. Available at: <http://www.referenceworld.com/sage/socialscience/triangulation.pdf>

Barker, S., (2020). *Surge in encrypted malware prompts warning about detection strategies*. Available at: <https://securitybrief.eu/story/surge-in-encrypted-malware-prompts-warning-about-detection-strategies>

Boyce, C. and Neale, P. (2006). *Conducting in-depth Interviews: A Guide for Designing and Conducting In-Depth Interviews*. Pathfinder International Tool Series

Bowling, A. and Ebrahim, S. (2005). *Handbook of Health Research Methods: Investigation, Measurement and Analysis*. Maidenhead, Berkshire: McGraw-Hill Education UK.

Bergman, M. (2008). *Advances in Mixed Methods Research: Theories and Applications*. London: Sage.

Berg, Bruce, L. and Howard L (2012). *Qualitative Research Methods for the Social Sciences*, 8th Edition. Harlow: Pearson.

Baadel, S., Thabtah, F. and Majeed, A. (2018) *Avoiding the Phishing Bait: The Need for Conventional Countermeasures for Mobile Users*. IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). DOI: [10.1109/ IEMCON.2018.8615095](https://doi.org/10.1109/IEMCON.2018.8615095)

Britz, M. (2013). *Computer forensics and cybercrime*. 3rd ed. Boston: Pearson.

Bryant, S. and Bryant, R. (2014). *Policing Digital Crime*. Farnham, Surrey: Ashgate Publishing Group.

Button, M., Lewis, C., and Tapley, J. (2009). *A better deal for fraud victims*. London: Centre for Counter Fraud Studies.

Bahnsen, A., Aouada, D., Stojanovic, A. and Ottersten, B. (2016). *Feature engineering strategies for credit card fraud detection*. *Expert Systems with Applications*, Volume 51, DOI: <https://doi.org/10.1016/j.eswa.2015.12.030>

Blog, (2016). *Survey reveals spear phishing as a top security concern to enterprises*. C.S. Blog.

Benenson, Z., Landwirth, R. and Gassmann, F. (2017). *Unpacking Spear Phishing Susceptibility*. University of Erlangen-Nürnberg and University des Saarlandes Germany.

Button, M and Cross, C. (2017). *Cyber Frauds, Scams and their Victims*. Abingdon, Oxon: Taylor and Francis. Available at: https://books.google.co.uk/books?id=GggqDwAAQBAJ&pg=PA205&dq=romance+fraud+prevention+strategies&hl=en&sa=X&ved=0ahUKEwi8kZ_Aks3gAhVxRBUIHRgYCQsQ6AEIKDAA#v=onepage&q=romance%20fraud%20prevention%20strategies&f=false

Button, M., Nicholls, C., Kerr, J. and Owen, R. (2014). *Online frauds: Learning from victims why they fall for these scams*. Australian and New Zealand Journal of Criminology, Volume 47, Issue 3. Available at:
<https://doi.org/10.1177/0004865814521224>

Bhattacharya, M. and West, J. (2016). *Intelligent financial fraud detection: A comprehensive review*. Computers and Security, Volume 57, DOI:
<https://doi.org/10.1016/j.cose.2015.09.005>

Bond, F. C. and DePaulo, M.B., (2006). *Accuracy of Deception Judgments of deception judgments, Personality and Social Psychology Review*. Volume 10, DOI: 10.1207/s15327957pspr1003_2

Boateng, Y.O.E., (2013). *Of Social Engineers and Corporate Espionage Agents: How Prepared Are SMEs in Developing Economies?* Journal of Electronics and Communications Engineering Research (JECER). Volume 1, no. 3.

Belson, D. (2018). *Finding Yourself: The Challenges of Accurate IP Geolocation*. Available at: <https://dyn.com/blog/finding-yourself-the-challenges-of-accurate-ip-geolocation/>

Barbour, R. and Flick, U., (2018). *Doing Focus Groups*. 2nd ed. United Kingdom: Sage.

Brownlee, J. (2017). *Gentle Introduction to the Adam Optimization Algorithm for Deep Learning*. Available at: <https://machinelearningmastery.com/adam-optimization-algorithm-for-deep-learning/>

Culling C. (2019). *Which YARA rules rule: basic or advanced?*, SANS institute. Available at: <https://www.sans.org/reading-room/whitepapers/tools/paper/38560>

Cisco, (2021). *What Is Phishing?* Available at:
https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html

Cascavilla, G., Tamburri, D.A. and Heuvel, W.J.V.D (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers and Security*, Volume 105, Elsevier, DOI: <https://doi.org/10.1016/j.cose.2021.102258>

Callegaro, M., Manfreda, K. and Vehovar, V. (2015). *Web survey methodology*. London: Sage Publications.

Chauhan B. (2020). *20 Must- Know Hacking Terminologies To Safeguard Your Online Business from Hackers*. Available at: <https://www.getastra.com/blog/knowledge-base/hacking-terminologies/>

Carpenter, P. (2019). *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviours*. Indianapolis, Indiana: John Wiley and Sons.

Clifford, N., Cope, M., Gillespie, T. and French, S. (2016). *Key Methods in Geography*. London: Sage.

Cybenko G, Gani A and Thompson P, (2002). *Cognitive hacking: A battle for the mind*. IEEE Xplore, DOI: 10.1109/MC.2002.1023788

Callegaro, M., and Wells, T. (2008). *Do online respondents go the extra mile and take on inconvenient tasks?* Available at: http://www.knowledgenetworks.com/ganp/docs/Do-Online-Respondents-Go-the-Extra-Mile-and-Take-on-Inconvenient-Tasks_6-25-08.pdf.

Creswell, J. and Clark, V. (2007). *Designing and conducting mixed methods research*. London: SAGE Publications.

Compeau and Higgins, (1995). D.R. Compeau, C.A. Higgins *Computer self-efficacy: Development of a measure and initial test*. *MIS Quarterly*, Volume 19.

Cranor, L. and Garfinkel, S. (2005). *Security and Usability- Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly.

Chiew, K. L., Yong, K.S.C and Tan, C.L., (2018). *A survey of phishing attacks: Their types, vectors and technical approaches*. Elsevier, Volume 106, DOI: <https://doi.org/10.1016/j.eswa.2018.03.050>

Cross, C. and Richards, K. (2018). *Online fraud victims' experiences of participating in qualitative interviews*. Criminal Justice Studies, Volume 31, Issue 1, DOI: <https://doi.org/10.1080/1478601X.2017.1396217>

Cross, C. and Blackshaw, D. (2015). *Improving the Police Response to Online Fraud*. Policing. Volume 9, Issue 2. DOI: <https://doi.org/10.1093/police/pau044>

Casey., E. (2010). *Handbook of Digital forensics and Investigation*. The Obald's Road, London: Elsevier.

Carcillo, F., Dal Pozzolo, A., Le Borgne, Y., Caelen, O., Mazzer, Y. and Bontempi, G. (2018). *SCARFF : A scalable framework for streaming credit card fraud detection with spark*. Information Fusion, Volume 41, DOI: <https://doi.org/10.1016/j.inffus.2017.09.005>

Carneiro, N., Figueira, G. and Costa, M. (2017). *A data mining-based system for credit-card fraud detection in e-tail*. Decision Support Systems, Volume 95, DOI: <https://doi.org/10.1016/j.dss.2017.01.002>

Caldwell, T. (2013). *Spear-phishing: how to spot and mitigate the menace*. Computer Fraud and Security, Volume 2013, Issue 1, DOI: [https://doi.org/10.1016/S1361-3723\(13\)70007-1](https://doi.org/10.1016/S1361-3723(13)70007-1)

Cialdini R. B . (1984). *Influence: The Psychology of Persuasion*. New York: William Morrow.

Canterbury Christ Church University (2020). *FACTS AND FIGURES*. Available at: <https://www.canterbury.ac.uk/about-us/facts-and-figures/facts-and-figures.aspx>

Correa Bahnsen, A., Aouada, D., Stojanovic, A. and Ottersten, B. (2016). *Feature engineering strategies for credit card fraud detection*. Expert Systems with Applications, Volume 51, DOI: <https://doi.org/10.1016/j.eswa.2015.12.030>

Chin, T and Xiong, K. (2018). *Phishlimiter: A Phishing Detection and Mitigation Approach Using Software-Defined Networking*. Volume 6, ISSN: 2169-3536. Available at: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8387883>

Clarke, R.R., (1997). *Situational Crime Prevention: Successful Case Studies (2nd ed.)*. New York: Harrow and Heston. [ISBN 0-911577-39-4](#).

Canterbury Christ Church University (2013). *Email Policy, 2013*. Available at: <https://www.canterbury.ac.uk/students/docs/policy-zone/email.pdf>

Canterbury Christ Church University (2016). *Guidance on the IT Regulations*. Available at: <https://www.canterbury.ac.uk/students/docs/policy-zone/core-regulations-guidance.pdf>

Ciena (2021). *What is SDN?* Available at: <https://www.ciena.com/insights/what-is/What-Is-SDN.html>

Davis, R., Lurigio, A. and Herman, S. (2013). *Victims of crime*. Thousand Oaks: SAGE Publications.

Davinson, N. and Sillence, E. (2010). *It won't happen to me: Promoting secure behaviour among internet users*. Computers in Human Behaviour, Volume 26, Issue 6, DOI: <https://doi.org/10.1016/j.chb.2010.06.023>

Dearden, L (2020). *'Radical' reform needed for police to cope with modern crime and security threats, report finds*. Available at: <https://www.independent.co.uk/news/uk/home-news/police-reform-crime-security-report-43-forces-a9642666.html>

Drake, T.N.C. (2016). *Mutual authentication security system with detection and mitigation of active man-in-the-middle browser attacks, phishing, and malware and other security improvements*. US, Available at:

<https://patents.google.com/patent/US10574692B2/en>

Doig, A. and Levi, M. (2009). *Inter-agency work and the UK public sector investigation of fraud, 1996–2006: joined-up rhetoric and disjointed reality*. Policing and Society, Volume 19, Issue 3, DOI: <https://doi.org/10.1080/10439460902863311>

Doig, A. (2018). *Fraud: from national strategies to practice on the ground—a regional case study*. Public Money and Management, Volume 38, Issue 2, DOI: <https://doi.org/10.1080/09540962.2018.1407164>

Daeef, M.M.A. and Saudi M.M. (2020). *URL's Folder Name Length as a Phishing Detection Feature*. Advances in Intelligent Systems and Computing, Volume 1184, Springer, Singapore. DOI: https://doi.org/10.1007/978-981-15-5859-7_32

Davidoff, S. and Ham, J., (2012). *Network Forensics: Tracking Hackers Through Cyberspace*. Upper Saddle River, NJ: Prentice Hall.

D. K. McGrath, M. and Gupta (2008). *Behind Phishing: An Examination of Phisher Modi Operandi*. Computer Science Department, Indiana University, Bloomington, in USA, Available at:

http://static.usenix.org/legacy/events/leet08/tech/full_papers/mcgrath/mcgrath.pdf

Davis, (1989). *F.D. Davis Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, Volume 13, Issue 3.

Dudovskiy, J. (2017). *Interpretivism (interpretivist) Research Philosophy*. Available at: <https://research-methodology.net/research-philosophy/interpretivism/>

Diksha, G. and Ankit, K.J., (2017). *Smishing-classifier: a novel framework for detection of smishing attack in mobile environment*. NGCT.

Debois, S. (2019). *10 Advantages and Disadvantages of Questionnaires*. Available at: <https://surveyanyplace.com/questionnaire-pros-and-cons/>

Doupé, A., Oest, A., Safei, Y., Ahn G.J., Wardman, B. and Warner, G. (2018). *Inside a Phisher's Mind: Understanding the Anti-phishing Ecosystem Through Phishing Kit Analysis*. Conference: 2018 APWG Symposium on Electronic Crime Research (eCrime), DOI: 10.1109/ECRIME.2018.8376206

Digital Marketplace (2020). *PurplePhish Avatu Ltd*. Available at: <https://www.digitalmarketplace.service.gov.uk/g-cloud/services/981297854887111>

Dhamija, R. Tygar, J.D. and Hearst, M. (2006). *Why phishing works?* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM

Denzin, K. N and Lincoln, S. Y., (1998). *The Landscape of Qualitative Research: Theories and Issues*, Sage Publications. Available at: https://www.researchgate.net/profile/Thomas_Schwandt/publication/232477264_Constructivist_Interpretivist_Approaches_to_Human_Inquiry/links/557048d908aeab777228bfef/Constructivist-Interpretivist-Approaches-to-Human-Inquiry.pdf

Duggleby, W. (2005). *What about focus group interaction data?* Qualitative Health Research, Volume 15.

Denzin N (1970). *The research act*. Chicago, Aldine.

Dawson, C. (2007). *Practical Research Methods*. Magdalen Road, Oxford: Howtobooks.

Dhamija, R., Tygar, J.D., and Hearst, M. (2006). *Why phishing works*. Proceedings of the CHI Conference on Human Factors in Computing Systems.

De Sá, A., Pereira, A. and Pappa, G. (2018). *A customised classification algorithm for credit card fraud detection*. Engineering Applications of Artificial Intelligence, Volume 72, DOI: <https://doi.org/10.1016/j.engappai.2018.03.011>

Dillard, J.P. and Pfau, M. (2002). *The Persuasion Handbook: Developments in Theory and Practice*. Sage, Thousand Oaks, CA.

Daejoong, K and Kim, H.J., (2013). *Understanding persuasive elements in phishing e-mails: A categorical content and semantic network analysis*. Online Information Review, Volume 37, Issue 6, DOI: <https://doi.org/10.1108/OIR-03-2012-0037>

Erickson, F. (1986). *Qualitative methods*. In M.C. Wittrock (Ed.), Handbook of research on teaching 3rd ed., New York: Macmillan

Europol (2017). *Current threats*. Available at: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime>

Edwards, R. and Holland, J. (2013). *What is qualitative interviewing?* London: Bloomsbury.

Europol (2020). *Cybercrime*. Available at: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime>

Europol (2019). *Spear Phishing A Law Enforcement and Cross-Industry Perspective*.

Europol (2020). *Internet Organised Crime Threat Assessment (IOCTA)*.

Europol (2014). *The Internet Organised Crime Threat Assessment (IOCTA)*.

Europol (2020) *Catching the virus cybercrime, disinformation and the COVID-19 pandemic*.

Europol (2020). *CYBERCRIME*. Available at: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime>

Europol (2020). *ABOUT EUROPOL*. Available at: <https://www.europol.europa.eu/about-europol>

Economic Times (2020). *Definition of 'Computer Virus'*. Available at: <https://economictimes.indiatimes.com/definition/computer-virus>

Europol (2020). *High-Tech Crime*. Available at: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime>

Erdal, O., and Islam (2019). *Inside the Dark Web*. CRC Press, Taylor and Francis Group, London.

Emigh, A., (2006). *The Crimeware Landscape: Malware Phishing, Identity Theft and Beyond*. Journal of Digital Forensic Practice, Volume 1, Issue 3.

Experian (2015). *5 of the most remarkable instances in the history of fraud*. Available at: <https://www.experian.co.uk/blogs/latest-thinking/identity-and-fraud/5-of-the-most-remarkable-instances-in-the-history-of-fraud/>

Exploit Development (2016). *Most Exploited Vulnerabilities: by Whom, When, and How*. Available at: <https://resources.infosecinstitute.com/most-exploited-vulnerabilities-by-whom-when-and-how/>

Ferguson, J., A. (2005). *Fostering E-Mail Security Awareness: The West Point Carronade*. Educause Quarterly, Volume 28, Issue 1. Available at: <https://www.learntechlib.org/p/103686/>

F-Secure (2021). *Email-Worm*. Available at: <https://www.f-secure.com/v-descs/email-worm.shtml>

Fowler, J. and Floyd J. (1995). *Improving survey questions: Design and evaluation*. Volume 38. Thousand Oaks, CA: Sage Publications.

Furnell, S. (2013). *Still on the hook: the persistent problem of phishing*. Computer Fraud and Security, Volume 2013, Issue 10, DOI: [https://doi.org/10.1016/S1361-3723\(13\)70092-7](https://doi.org/10.1016/S1361-3723(13)70092-7)

Fox, K and Cook, C. (2011). *Is knowledge power? The effects of a victimology course on victim blaming*. Journal of Interpersonal Violence, Volume 26, Issue 17

Foozy, C.F.M., Ahmad, R. and Abdollah, M.F. (2013). *Phishing detection taxonomy for mobile device*. International Journal of Computer Science, Volume 10, Issues (IJCSI)

Federal Bureau of Investigation (FBI)/Internet Crime Complaint Centre. (2017). *2016 internet crime report*. Washington, DC: FBI. Available at: https://scholar.google.com/hl=en&publication_year=2017&author=Federal+Bureau+of+Investigation%2FInternet+Crime+Complaint+Center&title=2016+internet+crime+report

Fraud Watch International (2016). *What are... Phishing Kits?* Available at: <https://fraudwatchinternational.com/all/what-are-phishing-kits/>

Fruhlinger (2020). *What is phishing? How this cyber attack works and how to prevent it*, CSO from IDG Communications, Inc. Available at: <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

FSB (2020). *The act of phishing*. Available at: <https://www.fsb.org.uk/resources-page/the-act-of-phishing.html>

Furnell S.M., Bryant P. and Phippen AD (2007). *Assessing the security perceptions of personal Internet users*. Computer Security. Volume 26, Issue 5. DOI: 10.1016/j.cose.2007.03.001.

Furnell, S.M., (2007). *Phishing can we spot the signs?* Computer Fraud and Security.

Fraley, J.B., (2017). *Improved Detection for Advanced Polymorphic Malware*. Nova Southeastern University, College of Engineering and Computing,

Goldschlag D., Reed M., Syverson P. (1999.) *Onion Routing for Anonymous and Private Internet Connections*, Onion Router.

Grønkjær, M., Curtis, T., de Crespigny, C. and Delmar, C. (2011). *Analysing group interaction in focus group research: impact on content and the role of the moderator*. Volume 2, Issue 1.

Gass, R.H. and Seiter, J.S. (2007). *Persuasion, Social Influence, and Compliance Gaining*. Pearson, Boston, MA.

Grandahi, J., Gini Scott, G. and Littlefield, R. (2017). *Preventing Credit Card Fraud: A Complete Guide For Everyone from Merchants to Consumers*. Rowman and Littlefield Publishers, Inc.

Glabbeek, V.J., (2019). *Smishing: the new SMS fraud*. Available at: <https://www.techradar.com/uk/news/smishing-the-new-sms-fraud>

Goel, S., Williams, K. and Dincelli, E. (2017). *Got Phished? Internet Security and Human Vulnerability*. Journal of the Association for Information Systems, Volume 18, Issue 1

Gunikhan, S. and Kuppusamy S.K., (2018). *SmiDCA: An Anti-Smishing Model with Machine Learning Approach*. The Computer Journal. Volume 61, Issue 8, DOI: [https:// doi.org/10.1093/comjnl/bxy039](https://doi.org/10.1093/comjnl/bxy039)

Guba, E.G. and Lincoln, Y.S. (1994). *Competing paradigms in qualitative research, in N.K. Denzin and Y.S. Lincoln (eds), Handbook of Qualitative Research*. Thousand Oaks, CA: Sage.

Grix, J. (2010). *The Foundations of Research*. 2nd ed. Basingstoke, Hampshire: Palgrave Macmillan.

Goles, T. and Hirschheim, R. (2000). *The Paradigm is dead, the Paradigm is dead...long live the paradigm: The legacy of Burrell and Morgan*. The International Journal of Management Science, Volume 28.

Green, J. and Hart, L. (1994). *The Impact of Context on Data in Developing Focus Group Research*. Sociology of Health and Illness, Volume 16.

Greenbaum, T., (1998). *The Handbook For Focus Group Research*. 2nd ed. London: Sage.

Gill, P., Stewart, K., Treasure, E. and Chadwick, B. (2008). *Methods of data collection in qualitative research: interviews and focus groups*. British Dental Journal, DOI: <https://doi.org/10.1038/bdj.2008.192>

Goutal, S. (2019). *The emergence of image manipulation in phishing attacks*. Vade Secure. Available at: <https://www.vadesecure.com/en/blog/detecting-logos-in-phishing-attacks>

Giandomenico, N. (2020). *What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing*. DATAINSIDER, Digital Guardian's Blog. Available at: <https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing>

Holt, T., Bossler, A. and Seigfried-Spellar, K. (2015). *Cybercrime and Digital Forensics: An Introduction*. Abingdon, Oxon: Routledge.

Halkier, B. (2010). *Focus groups as social enactments: integrating interaction and content in the analysis of focus group data*. Volume 10, Issue 1.

Heron, S., (2007). *Botnet command and control techniques*. Network Security. (4): 13–16. doi:10.1016/S1353-4858(07)70045-4

Holt, T. and Lampke, E. (2010). *Exploring stolen data markets online: products and market forces*. Criminal Justice Studies. Volume 23, Issue 1, DOI: <https://doi.org/10.1080/14786011003634415>

Hardré P.L., Crowson, H.M., Xie, K. and Ly, C. (2006). *Testing differential effects of computer-based, web-based and paper-based administration of questionnaire research instruments*. British Journal of Educational Technology (BJET), DOI: <https://doi.org/10.1111/j.1467-8535.2006.00591.x>

Hennink, M. (2014). *Understanding focus group discussions*. New York: Oxford University Press.

House, E.R. (1994). *Integrating the qualitative and quantitative in C.S. Reichardt and S.F. Rallis (eds), The Qualitative-Quantitative Debate: New Perspectives*. Thousand Oaks, CA: Sage.

Halkier, B. (2010). *Focus groups as social enactments: integrating interaction and content in the analysis of focus group data*. Qualitative Research. Volume 10, Issue 1

Hancock, M.E., Amankwaa, L., Revell, M. A., Mueller, D. (2016). *Focus group data saturation: A new approach to data analysis*. The Qualitative Report, Volume 21, Issue 11.

Holtfreter, K., Reisig, D.M. and Pratt C.T., (2008). *LOW SELF-CONTROL, ROUTINE ACTIVITIES, AND FRAUD VICTIMISATION*. DOI: <https://doi.org/10.1111/j.1745-9125.2008.00101.x>

Hämmerli, B. and Sommer, R. (2007). *Detection of Intrusions and Malware, and Vulnerability Assessment*. Berlin: Springer.

Harris, C. (1997). *Developing online market research methods and tools, Paper presented to ESOMAR Worldwide Internet Seminar*. Lisbon. Available at: <http://www.metamorphlab.com/lisbon-paper.html>

Home Office (2020). *Fraud, Home Office Counting Rules For Recorded Crime*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881505/count-fraud-apr2-2020.pdf

Hu, J., Zhang, X., Ji, Y., Yan, H., Ding, L., Li, J. and Meng, H. (2016). *Detecting phishing websites based on the study of the financial industry webserver logs*. In: 2016 3rd international conference on information science and control engineering (ICISCE), pp 325–328. DOI: <https://doi.org/10.1109/icisce.2016.79>

Harrison, B., Svetieva, E. and Vishwanath, A (2016). *Individual processing of phishing emails: How attention and elaboration protect against phishing*. Online Information Review, Volume 40, Issue 2, DOI: <https://doi.org/10.1108/OIR-04-2015-0106>

Hutchins, E.M., Cloppert, M.J. and Amin R.M. (2011). *Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains*. Available at: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>.

HYPR (2021). *Script Kiddie*. Security Encyclopaedia. Available at: <https://www.hypr.com/script-kiddie/>

Hanna, R., Weinberg, B., Dant, R. and Berger, P.D. (2005). *Do internet-based surveys increase personal self-disclosure?* J Database Mark Cust Strategy Management, Volume 12, DOI: <https://doi.org/10.1057/palgrave.dbm.3240270>

Hadnagy, C., Fincher, M. and Dreeke, R. (2015). *Phishing Dark Waters : The Offensive and Defensive Sides of Malicious Emails*. John Wiley and Sons, Incorporated.

Hadnagy, C. (2018). *Social Engineering : The Science of Human Hacking*. Second Edition. John Wiley and Sons, Incorporated, Indianapolis, Indiana.

Innes, M. (2004). *Reinventing Tradition?* Criminal Justice. Volume 4, Issue 2, DOI: [https:// doi.org/10.1177/1466802504044914](https://doi.org/10.1177/1466802504044914)

Interpol (2019). *Payment card fraud INTERPOL*. [online] Available at: <https://www.interpol.int/Crimes/Financial-crime/Payment-card-fraud>

Interpol (2020). *COVID-19 fraud schemes*. [online] Available at: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19>

Interpol (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>

Interpol (2020). *Social engineering scams*. [online] Available at: <https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams> [Accessed 13th July 2020].

Interpol (2020). *Cybercrime threat response*. [online] Available at:
<https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-threat-response>

Interpol (2020). *What is INTERPOL?*. [online] Available at:
<https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>

Interpol (2014). *INTERPOL strengthens cooperation with Kaspersky Lab in global fight against cybercrime*. Available at: <https://www.interpol.int/en/News-and-Events/News/2014/INTERPOL-strengthens-cooperation-with-Kaspersky-Lab-in-global-fight-against-cybercrime>

Islam, R. and Ozkaya, E., (2019). *Inside The Dark Web*. 6000 Broken Sound Parkway: CRC Press, Taylor and Francis Group.

Irwin, L. (2020). *5 ways to detect a phishing email – with examples*. IT Governance Blog. Available at: <https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email>

Ivankova, N. (2014). *Mixed methods applications in action research*. London: Sage Publications.

Iacovos, K., and Sasse, A. M. (2012). *Security Education against Phishing: A Modest Proposal for a Major Rethink, Security and Privacy, IEEE*. Volume 10, Issue 2, DOI: 10.1109/MSP.2011.179

Imperva (2020). *Phishing attacks*. Available at:
<https://www.imperva.com/learn/application-security/phishing-attack-scam/>

Information Commissioner's Office (2019). *Report a breach*. [online] Available at:
[https:// ico.org.uk/for-organisations/report-a-breach/](https://ico.org.uk/for-organisations/report-a-breach/)

IBM (2019). *2019 Cost of a Data Breach Report*. Available at:
<https://www.ibm.com/security/data-breach>

Ismail, A., Khawandi, S. and Abdallah, F. (2019). *Image Spam Detection: Problem and Existing Solution*. International Research Journal of Engineering and Technology, Volume 6, Issue 2.

Ippolito, P.P. (2019). *Stochastic Processes Analysis. An introduction to Stochastic processes and how they are applied every day in Data Science and Machine Learning*. Towards Data Science. Available at:

<https://towardsdatascience.com/stochastic-processes-analysis-f0a116999e4>

Ivanov, M. A., Kliuchnikova, B. V., Chugunkov I. V. and Plaksina, A. M. (2021). *Phishing Attacks and Protection Against Them*. 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, Moscow, Russia. DOI: 10.1109/EIConRus51938.2021.9396693.

Jansson, K. and Solms Von, R. (2013). *Phishing for phishing awareness*. Taylor and Francis Online, Volume 32, Issue 6, DOI:

<http://dx.doi.org/10.1080/0144929X.2011.632650>

Jagatic, T., Johnson, N., Jakobsson, M. and Menczer, F. (2007). *Social phishing*. Communications of the ACM, Volume 50, Issue 10, available at:

<http://www.markus-jakobsson.com/papers/jakobsson-commacm07.pdf>

Joyce, P. (2011). *Policing*. London: SAGE.

Jain, A. K. and Gupta, B. B. (2017). *Phishing detection: analysis of visual similarity based approaches*. Security and Communication Networks, volume. 2017

Johnson, M. (2013). *Cyber Crime, Security and Digital Intelligence*. Farnham, Surrey: Gower Publishing Limited

Jackson, B. (2020). *Email Authentication – Don't Let Your Emails End Up in Spam*. Available at: <https://kinsta.com/blog/email-authentication/#email-authentication>

Johnson, R., (2020). *Social Engineering And Information Warfare Operations: Emerging Research And Opportunities*. IGI Global.

Jakobsson, M. , Tsow, A. , Shah, A. , Blevis, E. and Lim, Y.K. (2007). *What instills trust? A qualitative study of phishing*. Lecture Notes in Computer Science, Volume 4886. Springer Verlag, Heidelberg

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P., He-Guelton, L. and Caelen, O. (2018). *Sequence classification for credit-card fraud detection*. Expert Systems with Applications. Available at: <https://doi.org/10.1016/j.eswa.2018.01.037>

Jernigan, S. and Meyers, M. (2018). *Mike Meyers' CompTIA Security+ Certification Guide, Second Edition (Exam SY0-501)*. 2nd ed. San Francisco: McGraw-Hill Education.

Joelianto, E. (2021). *Cyber Physical, Computer and Automation System*. Springer

Kerr, J., Owen, R., McNaughton-Nicolls, C., and Button, M. (2013). *Research on Sentencing Online Fraud Offences*. London: Sentencing Council.

Kirda E. and Kruegel C. (2005). *Protecting Users Against Phishing Attacks with AntiPhish*. Publisher: IEEE. Available at: <https://ieeexplore.ieee.org/document/1510078/ authors#authors>

Kültür, Y. and Çağlayan, M. (2016). *Hybrid approaches for detecting credit card fraud*. Expert Systems, Volume 34, Issue 2, DOI: 10.1111/exsy.12191

Kumar, Y. and Subba, B. (2021). *A lightweight machine learning based security framework for detecting phishing attacks*. International Conference on Communication Systems and Networks (COMSNETS), Bangalore, India, DOI: 10.1109/COMSNETS51098.2021.9352828.

Kleitman S, Law MKH and Kay J (2018). *It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling*. PLoS ONE Volume 13, Issue 10: e0205089. Available at: <https://doi.org/10.1371/ journal.pone.0205089>

Kritzinger, E., and von Solms, S. H. (2013). *Home user security-from thick security-oriented home users to thin security-oriented home users*. Paper presented at the Science and Information Conference (SAI)

Kritzing and von Solms (2010). *Cyber security for home users: A new way of protection through awareness enforcement*. Computers and Security, Volume 29, Issue 8, DOI: <http://dx.doi.org/10.1016/j.cose.2010.08.001>

Kovacich, G. and Jones, A. (2006). *High-technology crime investigator's handbook*. 2nd ed. Burlington, MA: Butterworth-Heinemann.

Kitzinger, J. (1994). *The methodology of focus groups: the importance of interaction between research participants*. Sociology. Health illness. Volume 16, Issue 1

Kiernan, N. E., Kiernan, M., Oyler, M. A., and Gilles, C. (2005). *Is a web survey as effective as a mail survey? A field experiment among computer users*. American Journal of Evaluation, Volume 26, Issue 2.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F. and Hong, J. (2007). *Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer*. In APWG eCrime researchers' summit. Pittsburgh, PA, USA.

Kitzinger, J. (1995). *Introducing focus groups*. BMJ: British Medical Journal.

Krueger, R. A and Casey, M. A. (2000). *Focus groups: A practical guide for applied researchers* (3rd ed.). Thousand Oaks, CA: Sage

Kaspersky (2021). *Spam and phishing in 2020*. Available at: <https://securelist.com/spam-and-phishing-in-2020/100512/>

Kaspersky (2021). *How Cybercriminals Try to Combat and Bypass Antivirus Protection*. Available at: <https://www.kaspersky.com/resource-center/threats/combating-antivirus>

Kaspersky (2020). *What is a Keylogger?* Available at: <https://www.kaspersky.co.uk/resource-center/definitions/keylogger>

Kaspersky (2021). *What Is an Advanced Persistent Threat (APT)?* Available at: <https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats>

Kaspersky (2021). *What Is Vishing?* Available at:
<https://www.kaspersky.com/resource-center/definitions/vishing>

Kaspersky (2021). *What is Spear Phishing?* Available at:
<https://www.kaspersky.co.uk/resource-center/definitions/spear-phishing>

Kaspersky (2020). *Kaspersky VPN Privacy at lightspeed.* Available at:
<https://www.kaspersky.com/acq/vpn-generic>

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). *Protecting people from phishing: The design and evaluation of an embedded training email system.* In *SIGCHI conference on human factors in computing systems*. San Jose, California, USA.

Kastner, E. (2020). *What is Email Filtering and How Does it Work?* Available at:
<https://www.soscanhelp.com/blog/what-is-email-spam-filtering-and-how-does-it-work#what>

Kim, D. and Kim, H.J. (2013). *Understanding persuasive elements in phishing e-mails: a categorical content and semantic network analysis.*

Kitzinger, J. (1994). *The Methodology of Focus Groups: The Importance of Interaction between Research Participants.* *Sociology of Health and Illness*, Volume 16.

Kaur, S., Randhawa, S. (2020). *Dark Web: A Web of Crimes.* Wireless Personal Communications, Springer, DOI: <https://doi.org/10.1007/s11277-020-07143-2>

Keepnet Labs (2020). *Antivirus Tools Can't Stop Phishing Attacks.* Available at:
<https://www.keepnetlabs.com/antivirus-tools-cant-stop-phishing-attacks-anti-phishing-solution-that-can-stop-phishing-attacks/>

Keepnet Labs (2020). *What is Baiting?* Available at:
<https://www.keepnetlabs.com/baiting/>

Lea, S., Fischer, P. and Evans, K (2009). *The Psychology of Scams: Provoking and Committing Errors of Judgement report for the Office of Fair Trading*. Available at: [https:// www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf](https://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf).

Lazar, J., Feng, J. and Hochheiser, H. (2015). *Research methods in human-computer interaction*. Chichester: Wiley.

Lunn, E., (2020). Covid-19 'smishing' texts warning: UK Finance. Available at: <https://www.mortgagestrategy.co.uk/news/covid-19-smishing-texts-warning-uk-finance/>

Lazar J. and Preece, J. (2001). *Using electronic surveys to evaluate networked resources: From idea to implementation*. In C. McClure and J.Bertot (eds), *Evaluating Networked Information Services: Techniques, Policy, and Issues*, Medford, NJ: Information Today.

Liamputtong, P. (2011). *Focus Group Methodology: Principle and Practice*. London: SAGE.

Layder, D. (2018). *Investigative research-Theory and Practice*. London: Sage Publications Ltd.

Larkin M, Watts S and Clifton E. (2006). *Giving voice and making sense in interpretative phenomenological analysis*. *Qualitative Research Psychology*, Volume 3, Issue 2, DOI: 10.1191/1478088706qp062oa

Liamputtong, P. (2011). *Focus Group Methodology: Principle and Practice*. London: Sage.

Litosseliti, L. (2010). *Research methods in linguistics*. London: Bloomsbury Publishing.

Logsign (2020). Why Social Engineering Are Major Threats in 2020? Introduction. Available at: <https://blog.logsign.com/why-social-engineering-are-major-threats-in-2020/>

Li, L. and Helenius, M. (2007). *Usability evaluation of anti-phishing toolbars*. Journal in Computer Virology. Volume 3, No. 2.

Leech, L. N., Dellinger, B. A., Brannagan, B. K., Tanaka, H. (2010). *Evaluating Mixed Research Studies: A Mixed Methods Approach*. Journal of Mixed Methods Research, Volume 4, Issue 1, Sage, DOI: 10.1177/1558689809345262. Available at: [https:// journals.sagepub.com/doi/pdf/10.1177/1558689809345262](https://journals.sagepub.com/doi/pdf/10.1177/1558689809345262)

Lam, T. and Kettani, H. (2018). *PhAttApp: A Phishing Attack Detection Application*. The Beacom College of Computer and Cyber Sciences, Dakota State University, Madison, South Dakota and USA Orange County Water District, Fountain Valley, California, USA

Loveday, B. (2017). *Still plodding along? The police response to the changing profile of crime in England and Wales*. International Journal of Police Science and Management. Volume 19, Issue 2. Sage, Institute of Criminal Justice Studies, University of Portsmouth, UK, DOI: 10.1177/1461355717699634

Love, J. (2017). *Top 10 Malicious Email Threats*. Available at: <https://www.lastline.com/blog/top-10-malicious-email-threats/>

Lietz P. (2010). *Research into Questionnaire Design: A Summary of the Literature*. International Journal of Market Research. DOI:10.2501/S147078530920120X

Lakshmi, L., Reddy, M.P., Santhaiah, C. and Reddy, U.J. (2021). *Smart Phishing Detection in Web Pages using Supervised Deep Learning Classification and Optimization Technique ADAM*. Wireless Personal Communication. Springer Nature Switzerland AG. DOI: <https://doi.org/10.1007/s11277-021-08196-7>

Laskowski, N. (2018). *Recurrent Neural Networks*. Pattern recognition and machine learning. TechTarget. Available at: <https://searchenterpriseai.techtarget.com/definition/recurrent-neural-networks>

Metropolitan Police (2021). *Cybercrime*. Online Fraud and Cybercrime. Available at: <https://www.met.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/>

Marshall, A. (2008). *Digital forensics*. Chichester, West Sussex: Wiley-Blackwell.

Mesch, G. and Dodel, M. (2018). *Low Self-Control, Information Disclosure, and the Risk of Online Fraud*. *American Behavioural Scientist*, Volume 62, Issue 10, DOI: [https://doi.org/ 10.1177/0002764218787854](https://doi.org/10.1177/0002764218787854)

Moore, R. (2011). *Cybercrime*. 2nd ed. Abingdon, Oxon: Routledge.

Mantzoukas, S., and Jasper, M. (2008). *Types of nursing knowledge used to guide care of hospitalised patients*. *Journal of Advanced Nursing*, Volume 62, Issue 3.

Manoranjitham, S., and Jacob, K. S. (2007). *Focus group discussion*. *Nursing Journal of India*, Volume 98, Issue 6.

Maxfield, M. and Babbie, E. (2017). *Research Methods for Criminal Justice and Criminology*. 8th ed. Boston: Cengage Learning.

Moore, T, and Clayton, R. (2007). *Examining the Impact of Website Take-down on Phishing*. Proceedings of the Anti-Phishing Working Group eCrime Researchers Summit, 1–13. Computer Laboratory, University of Cambridge.

Milletary, J. (2005). *Technical trends in phishing attacks*. US-CERT

Mehan, J., (2016). *Insider Threat*. Cambridge: IT Governance Ltd.

Malin, C., Casey, E. and Aquilina, J., (2012). *Malware Forensics Field Guide For Windows Systems: Digital Forensics Field Guides Digital Forensics Field Guides Malware Forensics Field Guide For Linux Systems Forensics 2011*. London: Elsevier.

Meland, H.P and Sindre, G. (2019). *Cyber Attacks for Sale*. Norwegian University of Science and Technology, International Conference on Computational Science and Computational Intelligence (CSCI), DOI:10.1109/CSCI49370.2019.00016. Available at: <https://american-cse.org/csci2019/pdfs/CSCI2019-14dQVW1stBtXVEInMQPd3t/558400a054/558400a054.pdf>

Moramarco, S., (2020). *Phishing Definition and History*. Infosec Resources 2020, available at:
<https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-definition-and-history/>

Mason, A., Watson, G. and Ackroyd (2014). *Social Engineering Penetration Testing Executing Social Engineering Pen Tests, Assessments and Defense*. Syngress, Elsevier Inc, DOI: <https://doi.org/10.1016/C2013-0-12926-1>

Mirea, M., Wang, V., & Jung J. (2019). *The not so dark side of the darknet: a qualitative study*. Security Journal, Volume 32, Springer, DOI:
<https://doi.org/10.1057/s41284-018-0150-5>

Malwarebytes (2021). *What is a spoofing attack?* Available at:
<https://www.malwarebytes.com/spoofing/>

McIntyre, L. J. (1999). *The practical skeptic: Core concepts in sociology*. Mountain View, CA: Mayfield Publishing.

Naidu, V., (2018). *Identifying Polymorphic Malware Variants using Biosequence analysis techniques*. University of Technology, New Zealand. Available at: https://www.researchgate.net/profile/Vijay-Naidu/publication/329415014_Identifying_Polymorphic_Malware_Variants_Using_Biosequence_Analysis_Techniques/links/5c36e239458515a4c71a3a9d/Identifying-Polymorphic-Malware-Variants-Using-Biosequence-Analysis-Techniques.pdf

Newburn, T. (2017). *Criminology*. 3rd ed. Abingdon, Oxon: Routledge.

Newman, R. (2010). *Computer security*. Sudbury, Massachusetts: Jones and Bartlett Publishers.

Norton (2018). *Norton Core Validates Need for Home Wi-Fi Network Security: More Than 90 Million Threats Blocked in First Year*. Available at: <https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2018/Norton-Core-Validates-Need-for-Home-Wi-Fi-Network-Security-More-Than-90-Million-Threats-Blocked-in-First-Year/default.aspx>

National Cyber Security Centre (2020). *NCSC glossary- The NCSC glossary - a set of straightforward definitions for common cyber security terms*. Available at: <https://www.ncsc.gov.uk/information/ncsc-glossary>

National Crime Agency (2020). *What is cyber crime?* Available at: <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices>

National Crime Agency (2020-2021). *Annual Plan 2020-2021- Leading the UK's fight to cut serious and organised crime*. Available at: <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/439-national-crime-agency-annual-plan-2020-2021-1/file>

National Crime Agency (2019). *National Strategic Assessment of Serious and Organised Crime (2019)*.

National Crime Agency (2020). *Fraud*. Available at: <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime>

National Cyber Security Centre (2016). *I'm Gonna Stop You, Little Phishie*. Available at: <https://www.ncsc.gov.uk/blog-post/im-gonna-stop-you-little-phishie>

National Security and Intelligence, Cabinet Office, HM Treasury and Hammond, P., (2016). *National Cyber Security Strategy 2016 to 2021*. [online] GOV.UK. Available at: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

National Cyber Security Centre (2020). *Experts at the NCSC have revealed phishing attacks exploiting worries over COVID-19*. Available at: <https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus>

National Cyber Security Centre (2018). *Phishing Attacks: Defending Your Organisation*. Available at: <https://www.ncsc.gov.uk/phishing>

National Crime Agency (2018). *National Strategic Assessment of Serious and Organised Crime*. Available at: <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/173-national-strategic-assessment-of-serious-and-organised-crime-2018/file>

National Crime Agency (2020). *Fraud*. Available at: <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime>

Nathezhtha, T., Sangeetha D. and Vaidehi, V., (2019). *WC-PAD: Web Crawling based Phishing Attack Detection*. International Carnahan Conference on Security Technology (ICCSST), CHENNAI, India.

National Institute of Standards and Technology (2018). *Framework for improving critical infrastructure cybersecurity*. National Institute of Standards and Technology, Gaithersburg.

Norton, (2020). *What is malware and how can we prevent it?* Available at: <https://uk.norton.com/internetsecurity-malware.html>

Nmachi, W.P. and Win, T., (2021). *Mitigating Phishing Attack in Organisation: A Literature Review*. School of Computing & Engineering University of Gloucestershire, Park Campus, Cheltenham. DOI: 10.5121/csit.2021.110105

Nyumba, T.O., Wilson, K., Derrick, C.J. and Mukherjee, N. (2018). *The use of focus group discussion methodology: Insights from two decades of application in conservation*. Volume9, Issue1, Special Feature: Qualitative methods for eliciting judgements for decision making. British Ecological Society.

Overink, F. J , Montoya, L. and Junger, M. (2017). *Priming and warnings are not effective to prevent social engineering attacks*. Computers in Human Behaviour, Volume 66, DOI: <https://doi.org/10.1016/j.chb.2016.09.012>

Orhan and Karyda (2017). *Employing Recent Technologies for Improved Digital Governance*. IGI Global, DOI: 10.4018/978-1-7998-1851-9.ch0

OASIS Cyber Threat Intelligence (2017). (CTI) TC STIX™ version 2.0. Part 2: STIX objects, OASIS Cyber Threat Intelligence (CTI) TC. Available at: http://docs.oasis-open.org/cti/stix/v2.0/cs01/part2-stix-objects/stix-v2.0-cs01-part2-stix-objects.html#_Toc496714313

Office for National Statistics (ONS) (2020). *Nature of crime: fraud and computer misuse*. Available at:
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse>

Our Community Pty Ltd (2020). *The A-Z of Technology Terms*. Available at: https://www.ourcommunity.com.au/tech/tech_article.jsp?articleId=74

Office for National Statistics (ONS) (2020). *Nature of fraud and computer misuse in England and Wales: year ending March 2019. Summary of the various sources of data for fraud and computer misuse and what these tell us about victims, circumstances and long-term trends*. Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#fraud-amount-and-type-of-loss-incurred>

Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis J., Zand, A., Thomas, K., Doupé, A. and Ahn G.J. (2020). *Sunrise to sunset: Analysing the end-to-end life cycle and effectiveness of phishing attacks at scale*. In Proceedings of the 29th USENIX Security Symposium.

Office of Cyber Security and Information Assurance in the Cabinet Office (2020). Cabinet Office, Detica. Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., and Butavicius (2011). *Why do some people manage phishing e-mails better than others?* University of Adelaide and Defence Science and Technology Organisation, Volume 20, Issue 1, DOI:
[https://doi.org/ 10.1108/09685221211219173](https://doi.org/10.1108/09685221211219173)

Puhakainen, P., and Siponen, M. (2010). *Improving employees' compliance through information systems security training: An action research study.* MIS Quarterly, Volume 34, Issue 4

Porter, K. (2020). *What is a rootkit? And how to stop them.* Available at:
<https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html>

Perrault, K., E (2018). *Using an Interactive Online Quiz to Recalibrate College Students' Attitudes and Behavioural Intentions About Phishing.* Journal of Educational Computing Research, Volume 55, Issue 8, DOI: 10.1177/07535633117699232, available at: [https:// journals.sagepub.com/doi/pdf/10.1177/07535633117699232](https://journals.sagepub.com/doi/pdf/10.1177/07535633117699232)

Peretti, K. K. (2008). *Data Breaches: What the underground world of 'carding' reveals.* Santa Clara Computer and High Technology Journal, Volume 25. Available at:
[https://](https://heinonline.org/HOL/LandingPage?handle=hein.journals/sccj25&div=16&id=&page)
heinonline.org/HOL/LandingPage?handle=hein.journals/sccj25&div=16&id=&page

≡

Plano Clark, V. and Ivankova, N. (2015). *Mixed Methods Research: A Guide to the Field of Mixed Methods.* Volume 3 Research Series. London: SAGE Publications.

Perloff, R.M. (2007). *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century.* Lawrence Erlbaum, Hillsdale, NJ.

Phishing Tackle (2021). *What is Spear Phishing?* Available at:
<https://www.phishingtackle.com/spear-phishing/>

Paltridge, B. (2006). *Discourse Analysis: An Introduction*. London: Continuum.

Pequegnat, W., Rosser, B.R.S. and Bowen, A.M. (2007). *AIDS Behaviour Conducting Internet-Based HIV/STD Prevention Survey Research: Considerations in Design and Evaluation*. Volume 11, Issue 4, DOI: <https://doi.org/10.1007/s10461-006-9172-9>

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C. (2015). *The design of phishing studies: Challenges for researchers*. Computer and Security, Elsevier, DOI: <https://doi.org/10.1016/j.cose.2015.02.008>

Purkait, S. (2012). *Phishing countermeasures and their effectiveness-literature review*. Emerald Group Publishing Limited, Information Management and Computer Security, Volume 20, DOI: 10.1108/09685221211286548

Patsakis, C. and Casino, F. (2019). *Hydras and ipfs: a decentralised playground for malware*. Elsevier, Computers and Security, Volume 88. DOI: <https://doi.org/10.1016/j.cose.2019.101614>

Phishing.org (2021). History of Phishing. KnowBe4, Inc. Available at: <https://www.phishing.org/history-of-phishing>

Phoka and Suthaphan, (2019). *Image Based Phishing Detection Using Transfer Learning*. 11th International Conference on Knowledge and Smart Technology (KST). IEEE, DOI:10.1109/KST.2019.8687615

Petty and Cacioppo, (1986). *The Elaboration Likelihood Model of Persuasion*. Advances in Experimental Social Psychology. Academic Press, Inc, DOI: 10.1016/S0065-2601(08)60214-2

Prakash, P., Kumar, M., Kompella R. R. and Gupta, M. (2010). *PhishNet: Predictive Blacklisting to Detect Phishing Attacks*. Proceedings of IEEE INFOCOM, San Diego, USA.

Pranav, C. (2020). *Cybersecurity issues and challenges faced in handling cybercrimes*. engrXiv by Cornell University, available at: <https://engrxiv.org/5chks/>

Phishing.org (2017). *What Is Phishing?* KnowBe4, Inc, available at: <https://www.phishing.org/what-is-phishing>

Ponulak, F. and Kasinski, A. (2010). *Supervised learning in spiking neural networks with ReSuMe: sequence learning, classification and spike-shifting*. Neural Computing. Volume 22, Issue 2, DOI:10.1162/neco.2009.11-08-901. PMID 19842989. S2CID 12572538.

Pickard, A.J. (2013). *Research Methods in Information*. Second Edition. Facet Publishing, London

Quah, J. and Sriganesh, M. (2008). *Real-time credit card fraud detection using computational intelligence*. Expert Systems with Applications, Volume 35, Issue 4, DOI: <https://doi.org/10.1016/j.eswa.2007.08.093>

Qabajeh I., Thabtah F., & Chiclana F. (2018). *A recent review of conventional vs. automated cybersecurity anti-phishing techniques*.

Roberts, L., (2008). *Cyber-Victimisation in Australia: Extent, Impact on Individuals and Responses*. University of Tasmania, Australia: Tasmanian Institute of Law Enforcement Studies. Available at: <http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan036070.pdf>

Rao, H. and Upadhyaya, S., (2009). *Information Assurance, Security And Privacy Services*. New York: Emerald Group Publishing.

Robson, C. (2002). *Real World Research*. Malden, MA: Blackwell Publishing.

Raheja, S., Munjal, G., Jangra, J. and Garg, R. (2021). *Rule-Based Approach for Botnet Behaviour Analysis*. Scrivener Publishing LLC, Wiley Online Library, DOI: <https://doi.org/10.1002/9781119711629.ch8>

Rosenstock, (1974). I.M. Rosenstock *The health belief model and preventive health behaviour*. Health Education Monographs, Issue 2

Rad, B.B., Masrom, M, and Ibrahim. S. (2012). *Camouflage in malware: from encryption to metamorphism*. International Journal of Computer Science and Network Security, Volume 12, Issue 8

Rad, B.B., Masrom, M, and Ibrahim. S. (2011). *Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey*. International Journal of Computer Science

Ross, B, Jackson, C, Miyake, N, Boneh, D. and Mitchell, C. J., (2005). *A Browser Plug- In Solution to the Unique Password Problem*. Available at: <http://crypto.stanford.edu/PwdHash/>

Rao, R.S., Vaishnavi, T. and Pais, A.R. (2020). *CatchPhish: detection of phishing websites by inspecting URLs*. Springer Nature Switzerland AG, DOI: <https://doi.org/10.1007/s12652-019-01311-4>

Reynolds, G., (2011). *Ethics In Information Technology*. 4th ed. Boston: Cengage Learning.

Robertson, C. (2013). *Indicators of compromise in memory forensics*. Available at: [https:// www.sans.org/reading-room/whitepapers/forensics/indicators-compromise-memory-forensics-34162](https://www.sans.org/reading-room/whitepapers/forensics/indicators-compromise-memory-forensics-34162)

RiskIQ (2019). *The Evil Internet Minute 2019*. Available at: <https://www.riskiq.com/resources/infographic/evil-internet-minute-2019/>

Rajaram J. and Dhasaratham M. (2021). *Scope of Visual-Based Similarity Approach Using Convolutional Neural Network on Phishing Website Detection*. In: Satapathy S., Bhateja V., Janakiramaiah B., Chen YW. (eds) Intelligent System Design. Advances in Intelligent Systems and Computing, vol 1171. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-15-5400-1_45

Rosenthai, M. (2021). *Must-Know Phishing Statistics: Updated 2021*. Available at: <https://www.tessian.com/blog/phishing-statistics-2020/>

Raphaely, E. (2020). *How to Prevent VPN Phishing Attacks*. Available at: <https://securityboulevard.com/2020/06/how-to-prevent-vpn-phishing-attacks/>

Romera, M. and Talatchian, P. (2018). *Vowel recognition with four coupled spin-torque nano-oscillators*.

Shipley, T. and Bowker, A (2014). *Investigating internet crimes- An Introduction to Solving Crimes in Cyberspace*. Waltham, MA: Syngress

Smithson, J. (2000). *Using and analysing focus groups: limitations and possibilities*. Social Research, Methodology, Volume 3, Issue 2

Saia, R. and Carta, S. (2019). *Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks*. Future Generation Computer Systems, DOI: <https://doi.org/10.1016/j.future.2018.10.016>

Symantec (2016). *Internet security threat report*. Available at: <https://docs.broadcom.com/doc/istr-21-2016-en>

Symantec (2019). *Internet security threat report*. Available at: <https://docs.broadcom.com/doc/istr-24-2019-en>

SecPoint (2021). *What is an Elite Hacker?* Available at: <https://www.secpoint.com/what-is-an-elite-hacker.html>

Sheikh A.F. (2020). *Attacks*. In: *CompTIA Security+ Certification Study Guide*. Apress, Berkeley, CA. DOI: https://doi.org/10.1007/978-1-4842-6234-4_9

Sophos (2019). *What's the Dark Web? What Happens There – and Is It All Illegal?* Available at: <https://home.sophos.com/en-us/security-news/2019/dark-web.aspx>

Sahin, Y., Bulkan, S. and Duman, E. (2013). *A cost-sensitive decision tree approach for fraud detection*. Expert Systems with Applications, Volume 40, Issue 15, DOI: <https://doi.org/10.1016/j.eswa.2013.05.021>

Senker, C. (2017). *Cybercrime and the Darknet- Revealing the Hidden Underworld of the Internet*. London: Arcturus Publishing Limited.

Saia, R. and Carta, S. (2019). *Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks*. Future Generation Computer Systems, Volume 93, DOI: <https://doi.org/10.1016/j.future.2018.10.016>

Stallings, W., Brown, L., Bauer, M. and Howard, M. (2012). *Computer security*. 2nd ed. Boston, Mass: Pearson.

Sarkar, K., (2018). *Cyber Security Botnet Attacks: Procedures And Methods*. Smashwords, Inc.

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L.F., and Hong, J.I. (2009). *Improving phishing countermeasures: An analysis of expert interviews*. In Proceedings of the Fourth Anti-Phishing Working Group eCrime Researchers Summit, Tacoma, WA.

Smith R. G. (2010). *Identity theft and fraud*. In: Jewkes Y., Yar M. (eds) *Handbook of internet crime*. Cullompton, England: Wiley

Smadi, S., Aslam, N. and Zhang, L. (2018). *Detection of online phishing email using dynamic evolving neural network based on reinforcement learning*. DOI: [https://doi.org/ 10.1016/j.dss.2018.01.001](https://doi.org/10.1016/j.dss.2018.01.001)

Sonowal, G. and Kuppusamy, S., K (2018). *SmiDCA: An Anti-Smishing Model with Machine Learning Approach*. The Computer Journal, Volume 61, Issue 8, DOI: [https:// doi.org/10.1093/comjnl/bxy039](https://doi.org/10.1093/comjnl/bxy039)

Summer, A., and Yuan X. (2019). *Mitigating Phishing Attacks: An Overview*. Kennesaw, GA, USA.

Saunders, M., Lewis, P. and Thornhill, A. (2012). *Research Methods for Business Students*. 6th edition, Pearson Education Limited

Sharp, H., Rogers, Y., and Preece J. (2007). *Interaction Design: Beyond human-computer interaction*. 2nd Edition, Chichester, UK: John Wiley and Sons.
Sue, V. and Ritter, L. (2007). *Conducting Online Surveys*. Los Angeles: Sage Publications.

Smith, JA. (1996). *Beyond the divide between cognition and discourse: using interpretative phenomenological analysis in health psychology*. Psychology Health. Volume 11, Issue 2, DOI: 10.1080/08870449608400256

Sale, J.E.M., Lohfeld, L.H. and Brazil, K. (2002). *Revisiting the Quantitative-Qualitative Debate: Implications for Mixed-Methods Research*. Kluwer Academic Publishers, Volume 36, Issue 43, DOI: <https://doi.org/10.1023/A:1014301607592>

Satpathy, S. and Mohanty, S., (2020). *Big Data Analytics And Computing For Digital Forensic Investigations*. Milton: CRC Press LLC.

Sudhakar and Kumar, S. (2020). *An emerging threat Fileless malware: a survey and research challenges*. Cybersecurity, Volume 3, Issue 1. DOI: <https://doi.org/10.1186/s42400-019-0043-x>

Stallings, W. and Brown, L. (2015). *Computer security*. Boston, Mass: Pearson.

Stewart (2006). *Analysing Focus Group Data*. London: Sage.

Swaminathan, R. and Mulvihill, T. (2017). *Critical approaches to questions in qualitative research*. Abingdon, Oxon: Routledge.

Schwartz–Shea, Yanow and Al (2013). *Interpretive research design: concepts and processes*. DOI: <https://doi.org/10.1080/13645579.2013.802464>

Salkind, N. (2012). *Triangulation*. *Encyclopaedia of Research Design*. DOI: [https:// dx.doi.org/10.4135/9781412961288.n469](https://dx.doi.org/10.4135/9781412961288.n469)

Sokolov, S., Nyrkov, A., Knysh, T. and Shvets A. (2021). *Countering Cyberattacks During Information Operations*. In: Mottaeva A. (eds) *Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020*. Lecture Notes in Civil Engineering, vol 130. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-33-6208-6_9

Saleeb, (2000). *J.R. Saleeb Health beliefs about mental illness: An instrument development study*. American Journal of Health Behaviour (24)

Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. (2010). *Who falls for phishing?: A demographic analysis of phishing susceptibility and effectiveness of interventions*. Proceedings of the 28th International Conference on Human Factors in Computing Systems—CHI'10 Available at:

<https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0171620>

Steinmetz, F.K. and Nobles, R.M. (2017). *Routine Activity Theory and Cybercrime A Theoretical Appraisal and Literature Review*. Routledge, New York, DOI:

<https://doi.org/10.4324/9781315117249>

Sim, J. and Waterfield, J. (2019). *Focus group methodology: some ethical challenges*. Qual Quant, Volume 53 <https://doi.org/10.1007/s11135-019-00914-5>

Smithson, J. (2000). *Using and analysing focus groups: limitations and possibilities*. Int. J. Soc. Res. Methodology. Volume 3, Issue 2

Srinivasa, R., Alwyn, R. and Pais R (2019). *Jail-phish: an improved search engine-based phishing detection*. Computer Security

Sira, R. (2003). *Network Forensics Analysis Tools: An Overview of an Emerging Technology*. Available at: <https://www.giac.org/paper/gsec/2478/network-forensics-analysis-tools-overview-emerging-technology/104303>

Sonowal, G. and Kuppusamy, K. S., (2018). *SmiDCA: An anti-smishing model with machine learning approach*. The Computer Journal. Volume 61, no. 8.

Sunil, A. N. V. and Sardana, A., (2012). *A PageRank based detection technique for phishing web sites*. IEEE Symposium on Computers and Informatics (ISCI).

Shaik, C. (2020). *Counter Challenge Authentication Method: A Defeating Solution To Phishing Attacks*. VISH Consulting Services Inc, Chicago IL, USA.

Scarpati, J. (2017). *Deep Packet Inspection (DPI)*. Available at:

<https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI>

Sameen, M., Han, K. and Hwang, S.O. (2020). *PhishHaven—An Efficient Real-Time AI Phishing URLs Detection System*. IEEE Access. Volume, 8. DOI: 10.1109/ACCESS.2020.2991403.

Shakela, V. and Jazri, H. (2019). *Assessment of Spear Phishing User Experience and Awareness: An Evaluation Framework Model of Spear Phishing Exposure Level (SPEL) in the Namibian Financial Industry*. 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Winterton, South Africa. DOI: 10.1109/ICABCD.2019.8851058.

Tajuddin, N., Dangi, M and Marzuki, S. (2016). *Fraudulent Short Messaging Services (SMS): Avoidance and Deterrence*. Regional Conference on Science, Technology and Social Sciences (2014). Springer, Singapore. DOI: https://doi.org/10.1007/978-981-10-1458-1_16

Tunggal, A.T., (2020). *What is a Cyber Threat?* Available at: <https://www.upguard.com/blog/cyber-threat>

Techopedia (2021). *What does Deep Neural Network mean?* Available at: <https://www.techopedia.com/definition/32902/deep-neural-network>

Tareek, M. and Sunil, B. (2015). *A Comparative Performance Evaluation of Content Based Spam and Malicious URL Detection in E-mail*. IEE, International Conference on Computer Graphics, Vision and Information Security (CGVIS).

Turanovic, C.T.P.J.J., Fox A.K and Wright., K (2013). *SELF-CONTROL AND VICTIMIZATION: A META-ANALYSIS*. DOI: <https://doi.org/10.1111/1745-9125.12030>

Tong, S. and Martin, D. (2016). *Introduction to Policing Research-Taking lessons from practice*. Abingdon, Oxon: Routledge.

Trenholm, S. (1989). *Persuasion and Social Influence*. Prentice Hall, Englewood Cliffs, NJ. todayadvisory (2020). *Reporting Fraud to the Police*. Available at: <https://www.todayadvisory.com/language-services/consultancy/reporting-fraud-to-the-police/>

Tixteco, M.D.C.P., Tixteco, L.P. Pérez, G.S and Toscano L.K. (2016). *Intrusion detection using Indicators of compromise based on best practices and windows event logs*. Cimp 2016: the eleventh international conference on internet monitoring and protection. Valencia, Spain

Tchakounté, F., Molengar, D. and Ngossaha, M.J (2020). *A Description Logic Ontology for Email Phishing*. Cameroon, International Journal of Information Security Science, Volume 9, No.1

Tashakkori, A., and Teddlie, C. (1998). *Mixed methodology: Combining qualitative and quantitative approaches*. Applied Social Research Methods, No.46. Thousand Oaks, CA: Sage.

Tandale, K. D. and Pawar S. N. (2020). *Different Types of Phishing Attacks and Detection Techniques: A Review*. International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India. DOI: 10.1109/ICSIDEMPC49020.2020.9299624.

Tashakkori A, Teddle C. (2003). *Handbook of mixed methods in social and behavioural research*. Thousand Oaks, CA: Sage.

The Tor Project (2018). *Introduction to Next Gen Onion Services (aka prop224 The Tor Project)*. 2018.

Tierney, S. (2018). *Protect yourself against the top 3 cyber threats of 2018*. Microsoft Industry Blogs, United Kingdom. Available at:
<https://cloudblogs.microsoft.com/industry-blog/en-gb/industry/financial-services/protect-yourself-against-the-top-3-cyber-threats-of-2018/>

Talamantes, J., (2014). *The Social Engineer's Playbook*. Woodbury, MN: Hexcode Publishing.

Tehrani, A.K.G. and Pontell, H.N. (2021). *Phishing Evolves: Analyzing the Enduring Cybercrime*. An International Journal of Evidence-based Research, Policy, and Practice, Volume 16, Taylor Francis Online. DOI:
<https://doi.org/10.1080/15564886.2020.1829224>

Thaware, V. (2020). *COVID-19 Outbreak Prompts Opportunistic Wave of Malicious Email Campaigns*. Symantec Enterprise Blogs/Threat Intelligence. Available at: <https://symantec-blogs.broadcom.com/blogs/threat-intelligence/covid-19-outbreak-prompts-opportunistic-wave-malicious-email-campaigns>

The Police Foundation (2018). *Fraud is not prioritised by the police, report finds*. Available at: <http://www.police-foundation.org.uk/news/policing-fraud/>

Terranova (2021). *What is Smishing?* Terranova Worldwide Corporation, available at: <https://terrانovasecurity.com/what-is-smishing/>

UK Finance (2020). *Fraud- The Facts 2020. The definitive overview of payment industry fraud*. Available at: <https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf>

Umarani, C. and Sengupta (2020). *Keyloggers: A Malicious Attack*. International Journal of Trend in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Volume 5, Issue 1. Available at: <https://www.searchdl.org/Resources/Public/Jnl/IJTSRD/5/1/ijtsrd35776.pdf>

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H. R. (2011). *Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model*. Decision Support Systems, Volume 51, DOI:10.1016/j.dss.2011.03.002

Vishwanath, A., Harrison, B and Ng, J., Y (2018). *Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility*. Communication Research, Volume 45, Issue 8, DOI:10.1177/0093650215627483

Vayansky, S. Kumar (2018). *Phishing challenges and solutions*. Computer Fraud Security.

Verizon (2015). *2015 Data Breach Investigations Report*. Available at: <https://msisac.cisecurity.org/whitepaper/documents/1.pdf>

Verizon (2020). *2020 Data Breach Investigations Report*. Available at:
<https://enterprise.verizon.com/en-gb/resources/reports/dbir/>

Verplanken, B. (1993). *Need for cognition and external information search: responses to time pressure during decision-making*. Journal of Research in Personality, Volume 27, No. 3.

Varshney, G., Misra, M. and Atrey, P.K. (2016). *A survey and classification of web phishing detection schemes*. Security and Communication Networks, Wiley Online Library. DOI: <https://doi.org/10.1002/sec.1674>

Van Buskirk, J., Naicker, S., Bruno, R.B., Breen, C. and Roxburgh, A. (2016). *Drugs and the Internet*. Issue 7. Australia: National Drug and Alcohol Research Centre.
VirusTotal Revision b9f925bb, (2019). *Welcome to YARA's documentation!*
Sphinx. Available at: <https://yara.readthedocs.io/en/v3.5.0/index.html>

Vigliarolo, B. (2021). *New malformed URL phishing technique can make attacks harder to spot*. ZDNET, A RED VENTURES COMPANY, TechRepublic.
Available at: <https://www.techrepublic.com/article/new-malformed-url-phishing-technique-can-make-attacks-harder-to-spot/>

Wang, J., Herath, T., Chen, R., Vishwanath, A. and Rao, H. (2012). *Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email*. IEEE Transactions on Professional Communication, Volume 55, Issue 4, DOI: 10.1109/TPC.2012.2208392

Which? (2020). *Hundreds of thousands of fraud reports delayed in police IT backlog An IT glitch at City of London Police stalled the processing of more than 300,000 crime reports, Which? Money has discovered* Available at:
<https://www.which.co.uk/news/2020/03/hundreds-of-thousands-of-fraud-reports-delayed-in-police-it-backlog/> - Which?

Wang, S. and Ledley, R. (2013). *Computer Architecture and Security: Fundamental of Designing Secure Computer Systems*. Singapore: John Wiley and Sons.

Wu, C., Kuo, C. and Yang, C. (2019). *A phishing detection system based on machine learning*. In: 2019 international conference on intelligent computing and its emerging applications (ICEA), Tainan, Taiwan, pp 28–32. DOI: <https://doi.org/10.1109/ICEA.2019.8858325>

Wang, J., Chen, R., Herath, T. and Rao, H.R (2009). *An exploration of the design features of phishing attacks*. H.R.R.S. Upadhyaya (Ed.), Information Assurance, Security and Privacy Services, Emerald Publishing Group.

Workman, M. (2008). *A test of intervention for security threats from social engineering*. Information Management and Computer Security, Volume 16, Issue 5

Williams, J.E and Joinson, N.A. (2020). *Developing a measure of information seeking about phishing*. Oxford Academic, Journal of Cybersecurity, Volume 6, Issue 1. DOI: <https://doi.org/10.1093/cybsec/tyaa001>

Williams, E. and Polage, D. (2019). *How persuasive is phishing email? The role of authentic design, influence and current events in email judgements*. Behaviour and Information Technology, Volume 38, Issue 2, DOI: <https://doi.org/10.1080/0144929X.2018.1519599>

Williams, E., Morgan, P. and Joinson, A. (2017). *Press accept to update now: Individual differences in susceptibility to malevolent interruptions*. Decision Support Systems, Volume 96, Available at: <https://doi.org/10.1016/j.dss.2017.02.014>

Wolcott, H. F. (1988). *Ethnographic research in education*. In R.M.Jaeger (Ed.), *Complementary methods for research in education*. Washington, DC: American Educational Research Association.

Warr (2005). *It was fun... but we don't usually talk about these things: analyzing sociable interaction in focus groups*. Volume 11, Issue 2

Wolcott , H. F. (1992). *Posturing in qualitative inquiry*. In M.D. LeCompte, W.L.Millroy, and J.Preissle. *The handbook of qualitative research in education*. New York: Academic Press.

Wright Rt, Charkraborty S, Basoglu A and Marett K (2010). *Where did they go right? Understanding the deception in phishing communications*. Group Decisions and Negotiation, Volume 19, Issue 4.

Winterfeld, S. and Andress, J. (2013). *The basics of cyber warfare*. Waltham, USA: Elsevier.

Warr, D (2005). *It was Fun...But We Don't Usually Talk about These Things: Analysing Sociable Interaction in Focus Groups*. Qualitative Inquiry, Volume 11, no. 2.

Wilkinson, S. (2004). *Focus group research*. In Silverman, D. (Ed.), *Qualitative research: Theory, method, and practice*. Thousand Oaks, CA: Sage

Wilkinson, S. (1998). *Focus groups in feminist research: power, interaction, and the co-production of meaning*. Women's Studies, International Forum, Volume 21, Issue 1

Weirich and Sasse, (2001). *Security and Usability- Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly.

Wu, M. , Miller, R.C. and Garfinkel, S.L. (2006). *Do security toolbars actually prevent phishing attacks?* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM Press, New York, NY.

Wu C.T., Cheng K.T., Qiang Z. (2005). *Using Visual features for anti-spam filtering*. Proc. IEEE International conference on Image Processing, Volume 3.

Workman, M. (2007). *Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security*. Journal of the American Society for Information and Technology, Volume 59, No. 4.

Xu Q., Xiang E., Du, J., Zhong., J and Yang, Q. (2012). *SMS spam detection using contentless features*. IEEE Intelligent Systems. Volume 99.

Xiujuan, W., Chenxi, Z., Kangfeng, Z., Haoyang, T. and Yuanrui, T. (2019). *Detecting spear-phishing emails based on authentication*. IEEE 4th International Conference on Computer and Communication Systems (ICCCS), Singapore. DOI: 10.1109/CCOMS.2019.8821758.

Yu, (2020). *Encyclopaedia of Criminal Activities and the Deep Web, Crime Hidden in Email Spam*. IGI Global, Wichita State University, USA, DOI: 10.4018/978-1-5225-9715-5.ch057

Yue, C. and Wang, H. (2008). *Anti-phishing in offense and defence*. Proceedings of the Annual Computer Security Applications Conference (ACSAC).

Yerima, Y.S and Alzaylaee K.M (2020). *High Accuracy Phishing Detection Based on Convolutional Neural Networks*. Cryptography and Security, Cornell University, available at: <https://arxiv.org/abs/2004.03960>

Yamin, M.M., Ullah, M., Ullah, H. and Katt, B. (2021). *Weaponised AI for cyber attacks*. Journal of Information Security and Applications. Volume 57. ScienceDirect, Elsevier. DOI: <https://doi.org/10.1016/j.jisa.2020.102722>

Zhang, Y., Egelman, S., Cranor, L and Hong, J. (2007). *Phinding phish: an evaluation of anti-phishing tools*. Proceedings of the ISOC Symposium on Network and Distributed System Security, Internet Society, San Diego, CA.

Zhang, Y., Hong, J. I and Cranor, L. F. (2007). *Cantina: a content-based approach to detecting phishing web sites*. Proceedings of the 16th international conference on Worldwide

Zhang, P., Oest A., Cho, H., Sun Z., Johnson, R., Wardman, B., Sarker, S., Kapravelos, A., Bao T., Wang, R., Shoshitaishvili, Y., Doupé, A. and Ahn, G.J. (2021). *CrawlPhish: Large-scale Analysis of Client-side Cloaking Techniques in Phishing*. Arizona State University, PayPal, Inc., North Carolina State University and Samsung Research. Available at: <https://zhbosun.me/publication/oakland2021/crawlphish-oakland21.pdf>

Zhang, H., Cheng, N. and Zhang, Y. (2021). *Label flipping attacks against Naive Bayes on spam filtering systems*. Applied Intelligence. DOI: <https://doi.org/10.1007/s10489-020-02086-4>

Appendix

Appendix A: Ethics Approval Letter

18th October 2019

Ref: 18/SAS/91C Nima

Movassagh

c/o School of Law, Criminal Justice and Policing,

Faculty of Social & Applied Sciences

Dear Nima,

Confirmation of ethics compliance for your study: *Gauging awareness levels of phishing emails from students at Canterbury Christ Church University and their perception of different types of phishing emails and their variants.*

The Faculty Ethics Chair has reviewed your Ethics Review Checklist application and appropriate supporting documentation for the above project. The Chair has confirmed that your application complies fully with the requirements for proportionate ethical review, as set out in this University's Research Ethics and Governance Procedures.

In confirming compliance for your study, you are reminded that it is your responsibility to follow, as appropriate, the policies and procedures set out in the *Research Governance Framework* ([http:// www.canterbury.ac.uk/research-and-consultancy/governance-and-ethics/governance-and-ethics.aspx](http://www.canterbury.ac.uk/research-and-consultancy/governance-and-ethics/governance-and-ethics.aspx)) and any relevant academic or professional guidelines. This includes providing, if appropriate, information sheets and consent forms, and ensuring confidentiality in the storage and use of data.

Any significant change in the question, design or conduct of the study over its course should be notified via email to red.resgov@canterbury.ac.uk and may require a new application for ethics approval.

It is a condition of compliance that you must inform red.resgov@canterbury.ac.uk once your research is complete.

Wishing you every success with your research.

Yours sincerely,

Ellen

Ellen Charman

Research Integrity & Development Officer

Email: red.resgov@canterbury.ac.uk

CC: Dr Paul Stephens, Supervisor

Research & Enterprise Integrity & Development Office Canterbury Christ Church University
North Holmes Campus, Canterbury, Kent, CT1 1QU Tel +44 (0)1227 767700 Fax +44 (0)1227
470442 www.canterbury.ac.uk Professor Rama Thirunamachandran, Vice Chancellor and
Principal

Registered Company No: 4793659 A Company limited by guarantee Registered Charity
No: 1098136

The study abided by the Canterbury Christ Church University Ethics principles. The study received approval from ethics the university ethics committee by contacting them via email with a completed a 'Ethics Review Checklist' application and supporting documentation relevant to the research such as the: consent form questionnaire and a blank copy of the questionnaire.

Appendix B: Data Protection Act (2018) and GDPR (2016) compliance in the study

The study ensured that participants responses in the anonymised questionnaire are anonymous and did not personally identify the participants in the research. The respondents were provided with information at the beginning of the questionnaire about consent to take part in the study. The individuals in the study given clear consent to process their anonymised personal data from the questionnaire and the focus group which was when respondents provided consent when asked if they wanted to take part in the research before the focus group started for a specific purpose of gauging the students awareness levels of different types of phishing. The anonymised questionnaire has a confidentiality section that included information about how the data and personal information of students in the study will be encrypted and stored securely in accordance with the Data Protection Act 2018, GDPR (2016) and the Canterbury Christ Church University's own data protection requirements. The anonymised data from the focus group and anonymised questionnaires from policing, criminology and computing students will be used to answer the research questions and make recommendations for further research in the future.

Appendix C: Consent Details

Title of Project: Awareness and perception of phishing variants from policing, computing and criminology students in Canterbury Christ Church University

Name of Researcher: Nima Movassagh

Contact details:

Address:

Canterbury Centre for Policing Research (CCPR),
Canterbury Christ Church University,
North Holmes Road,
Canterbury, Kent CT1 1QU

Tel: 0756405511 UNITED KINGDOM

Email: n.movassagh362@canterbury.ac.uk

By completing this survey, I agree to the following:

I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions.

I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason.

I understand that any personal information that you provide to me for my thesis will be kept strictly confidential.

TITLE: Awareness and perception of phishing variants from policing, computing and criminology students in Canterbury Christ Church University

Participant Information Sheet

Background

This research will survey students within the School of Law, Policing and Social Sciences at Canterbury Christ Church University. The research is about phishing and its variants.

What will you be required to do?

You are required to answer the questions on the questionnaire about phishing emails and its variants. Some questions will be about how you keep yourself safe online and if you use security measures on your: mobile phone, tablet, laptop and computer.

To participate in this research, you must:

Be a student at Canterbury Christ Church University and studying a criminology or policing course in the School of Law, Policing and Social Sciences.

Feedback and dissemination of results

You can request feedback via email about the questionnaire and questions about how the anonymised statistical information from the questionnaire will be included in the research project.

Confidentiality

All data and personal information will be stored securely within CCCU premises in accordance with the Data Protection Act 2018, General Data Protection Regulation (GDPR) and the University's own data protection requirements. All data from the questionnaire will be confidential (i.e., all of the responses from the questionnaire will be anonymous).

Deciding whether to participate

If you have any questions or concerns about the nature, procedures or requirements for participation do not hesitate to contact me. Should you decide to participate, you will be free to withdraw at any time without having to give a reason.

Any questions? Please contact:

Nima Movassagh from the School of Law, Policing and Social Sciences via email:
n.movassagh362@canterbury.ac.uk *I will be interested to speak to anyone who wished
to be interviewed at a later stage.*

Brief information about research: This questionnaire is about different types of phishing communication or emails you may receive on a day-to day basis.

***(Please note above background information about this research project is optional
to read)***



Appendix D: Questionnaire

1. UK Government websites provides advice and information for people about different types of fraudulent emails, text messages and calls you can receive from online criminals. Is the government doing enough to make users aware of phishing emails and their variants?

Please circle **one** of the following: or indicate that you are unsure below.

Yes— No— I do not know

Please provide a reason for your answer:

2. **Scenario:** You have received an email from a purchase you have made online for an item you have ordered during the Christmas period. The email contains general item information such as: the order number and date purchased. The email advises you to click on the link on the email to check the delivery progress of your item. Would you click on the link?

Please **circle one** of the following:

Yes— No

If you answered 'Yes' or 'No' **please explain your answer** or indicate that **you are unsure below.**

3. Have you received any phishing emails?

Please **circle one** of the following or indicate that you are unsure below.

Yes— No—I do not know

If you answered yes or no please explain how did you identify the email to be a phishing email?

4. What would you do if you receive a text from a delivery company (i.e., Royal Mail, FedEx, UPS, DPD or Hermes) for an item you have ordered online stating that you have to pay 0.50p delivery fees by following a link- <https://FedEx.org.uk/9991011110111> to receive the item today before 10:00AM, and the delivery ID in the text is #10010 and if the delivery fees are not paid in time then the item will be sent back to the sender.

What would you do next? Please explain your answer below.

Please provide a reason for your answer below

5. What would you do if you receive an email with an attachment?

Please provide a reason for your answer below

6. What precautions should you take to avoid phishing emails and their variants: 'SMiShing' (SMS phishing), Vishing, Spear Phishing and Pharming?

Please provide a reason for your answer below

7. **Scenario:** You have received an email from your PayPal account that your account has encountered an error in their system. In the email they say if this problem is not resolved, they will close your account. This is due to the account being inactive for some time. In the email PayPal mention that their verification process has encountered a technical problem because they are unable to verify your information. As a result, your account cannot function correctly and can lead to account deactivation.

What would you do next? Please explain your answer below.

8. Do you use security safeguards (firewalls and/or VPN-Virtual Private Network) on your electronic devices that you may use on a daily basis in order to prevent you from receiving different types of phishing communication via email, phone or from text messages?

Please **circle one** of the following or indicate that you are unsure below.

Yes— No—I do not know

Please provide a reason for your answer below

9. What would you do if you receive an urgent email from your bank which states that there's been fraudulent activity on your bankcard, so your account has been temporarily deactivated?

What would you do next? Please explain your answer below.

Please provide a reason for your answer below

Thank you for completing this questionnaire.

Appendix E: Question 2 Students Response Data.

1. I'm unsure.
2. I am unsure. I would only click on it if the email was the official site email.
3. I am unsure. Depending on whether the email was from the company I ordered the item from them I would but if it wasn't I wouldn't.
4. Yes. I would click on the link.
5. No. I wouldn't.
6. Yes. I will click the link to check the delivery of my item.
7. Yes. Yeah, I want to check the delivery process of my item.
8. No. I'll use the website I ordered from to track.
9. No. Most things I order I can track via other means or apps.
10. No. It's not necessary to click on the link as it could include something dodgy.
11. No. Because I am not usually that bothered when an item comes when I order unless it's very late. Also, because it may not be a real email from the person, I bought it from.
12. No. I don't need to know where the package is just long as I get it.
13. No. I never open email links, always go to the website.
14. No. As the email link may contain malware that then downloads onto your pc. But it would depend on the authenticity of the look of the email. To depend on whether I would think it was actually that company.
15. No. Never click on links to emails unless its sender is verified.
16. No. I don't tend to track my items unless they are late. I would then call or email the relevant people.
17. No. I usually sign up for text notification to have an email send through wouldn't look right.
18. No. Because you don't know what's on that link.

- 19.No. I wouldn't click on the link without being certain it is legit.
- 20.No. I always press the email address to see who has actually send the email.
- 21.No. Always weary of phishing emails.
- 22.No. Would only click on the link if the website was secure and had a lock.
- 23.No. I'll first search up on google to see if others receive emails such as this to ensure that it is legit.
- 24.No, I would check that the email address was legitimate first.
- 25.No. If it didn't look legitimate, I feel I would know. Also, I don't care about checking the delivery process usually.
- 26.No. I only usually click emails after dispatch where relevant info is given.
- 27.No. Because it could be a scam and could possibly be scammers obtaining your bank details, or personal information.
- 28.No. Because I would be very worried that it was a scam.
- 29.No. Because I didn't request any changes and would wait for the delivery I would only contact the company on non-delivery or not happy with product.
- 30.No. Because I don't need to and is a chance to be a scam.
- 31.No. Because I can check the progress on the website which I bought the item and not in my email.
- 32.No. Delivery process does not bother me, it arrives when it arrives.
- 33.No. Unless its directly from delivery company or order company.
- 34.No. Because the link is probably a virus and there is a chance at getting a virus to your phone. Also get your personal details and location. Especially if it's an iPhone and you have an apple pay, the virus can probably take the card details.
- 35.No. I don't click any link within my emails.
- 36.No. I would need more details to track the order.
- 37.No. I normally just wait for it to arrive.

38. Yes. Because I'd want to know the terms and conditions of the delivery process.
39. Yes. I probably wouldn't think anything of it unless it clearly looked dodgy.
40. Yes. if it seems to be the genuine company.
41. Yes. As long as it is a genuine email.
42. Yes. I would like to see how far away my parcel is and who's hands it is in.
43. Yes. If I bought the item. I want to check where it is.
44. Yes. Yes, if I knew it was definitely from the company I ordered from.
45. Yes. I expect it would be from a trusted source.
46. Yes. To find out when delivery is.
47. Yes. Only if I have pressed the link before on that specific website.
48. Yes. Because It contains 2 unique bits of information and its coming from an email address I recognise.
49. Yes. I would press the link if I was 100% sure that it was genuine.
50. Yes. I would want to track my parcel.
51. Yes. Because it's to track your parcel so usually there is nothing 'fishy' or criminal about doing that.
52. Yes. If bought it, I'd expect it to be what I ordered.
53. Yes. However, it depends if the email is legit from the usual email and if it looks secure.
54. Yes. Out of the panic I would check but only if the email seemed okay.
55. Yes. I would because it has the details of my purchase and during Christmas, I'd like to know the delivery progress.
56. Yes. Only if it was from the company, I bought it from.
57. Yes. Because it seems alright.
58. Yes. Paranoid that I'll be losing money.

59. Yes. If it was email from the company, I made the purchase from that contained the correct info and data then I would trust it.
60. Yes. So, you can track what stage your delivery is at.
61. Yes. If I had brought something from a trusted site, I would click on an email from them.
62. Yes. Always eager to see the progress on the delivery.
63. Yes. Expecting to be informed about the product ordered.
64. Yes. I would like to see where my delivery is if the sender looks legitimate, I would trust it.
65. Yes. Because having paid for the product I would want to know where it is.
66. Yes. Because I do online shopping and know the website do provide link to find out the delivery process of the purchase.
67. Yes. I would trust it was from the company as I had purchased the item.
68. Yes. As long as the notice seemed legitimate and professional. I would likely access it to be genuine.
69. Yes. I will have to check who email is from it is usually visible if email is fraudulent.
70. Yes. I always like to check my order's details and make sure I've been charged properly.
71. Yes. I would click the link because I would recognise that order most tracking links can be safe.
72. Yes, because I would like to know where the product I purchased is.
73. Yes. Because I would assume it was legit as I know I had purchased the item previously.
74. Yes. Yes, because it contains my order. Plus, if all my details were on there then it seems legit.
75. Yes. Yes, if the email address it is send from the company email and all the info is correct.

76. Yes. To be kept up to date with the delivery progress.
77. No. I wouldn't randomly click on an email. I would look at who it had been sent from to check its credibility. If I was unsure, I would just leave it.
78. Yes. We order a lot of things around Christmas time so I would check what it is, but if I had no memory of the purchase, I might check my bank statement first.
79. Yes. I want to know how far processed my order is and if it is out for delivery yet.
80. Yes. I would want to know the progress of my order.
81. Yes. To see when it would be delivered.
82. Yes. To see what's happening with the delivery. I wouldn't assume it's a scam.
83. Yes. I would click on the link to see the delivery progress of the item, but I would check the email address first etc as I would be unsure.
84. Yes. I would if it was a legit invoice or email confirmation of purchase made and your details were provided.
85. Yes. I wouldn't think anything strange about it and would want to track my delivery.
86. Yes. If it is a website I have bought off before, then I will click the link.
87. Yes. Why wouldn't you? You shouldn't have to suspect everything you receive is spam or not legit.
88. Yes. If it looks legitimate and I just ordered from that site I would.
89. Yes. I probably would, unless the email looked dodgy.
90. Yes. Cause I'd want to know when it would be delivered.
91. Yes. I'd like to know if my package has been shipped.
92. Yes. I would click the link in order to track my order and know when it is getting to me. I would also click the link because it has all the correct information on it and I trust it.
93. Yes. So, I can track my order.
94. Yes. I would want to see when my delivery is coming.

95. Yes. Need to find out about my order.
96. Yes. I would only check if it has not arrived after a prolonged period of time.
97. Yes. I always do because out of curiosity but only if it's for UPS, DPD, Royal Mail, Amazon or other 'big company'.
98. Yes. To track my parcel.
99. Yes. I have ordered item online and one of the steps I have to often take is to click on a link that keeps me up to date on the progress of my delivery.
100. Yes. I would believe it is legit as I ordered the item.
101. Yes. I would believe that due to the information being correct it would be genuine.
102. Yes. I usually track my deliveries so this wouldn't seem like an unusual email to receive.
103. Yes. The use of the order number etc. would lead me to believe it is legitimate.
104. Yes. If from the official website I would believe it wasn't a scam.
105. Yes. If it was a legit email.
106. Yes. Because I ordered the product.
107. Yes, because it was sent to my personal emails.
108. Yes. Yes, if the email is from the company and written correctly.
109. Yes. I want to know where my parcel is and I trust the stores I buy from.
110. Yes. If the email came from the company email address and all of the correct information.
111. Yes. If the email was from the company, I purchased the item from.
112. Yes, I would like to know where my order is. If I haven't received it yet.
113. Yes. I would click the link because if it contains my order number it would be legit.

114. Yes. As long as I am 100 per cent sure it's from the shop I ordered from. I would check senders email address first.
115. Yes. Seems like a legit email.
116. Yes. I trust the email.
117. Yes. So, I can track my delivery and make sure I will be home for it.
118. Yes. If it seems legit I would and if it was a purchase from a known website.
119. Yes. Only if the order numbers matched up and if I was aware, I had tracked delivery otherwise no I wouldn't.
120. Yes. This is because I am aware that it was sent by the company. And majority of websites let you track the delivery status like that.
121. Yes. I wouldn't have thought any differently about it as it always seems legitimate.
122. Yes. If I recognise the company in which I have ordered the item before then I will click it. If I don't recognise the company or haven't been notified that they will be delivery my order, then I won't click it.
123. Yes. If it is from the website, I purchased the item from I would check the tracking information to see how long the delivery takes.
124. Yes. If the email includes information regarding the order, I would assume the link would be legitimate.
125. Yes. To check my delivery order, I made.
126. Yes. I would like to be aware of where my parcel is and when it will be delivered.
127. Yes. Online receipts or a tracking page is usually sent so I would open it to track the parcel.
128. Yes. I would like to see the date it is expected to arrive.
129. Yes. If it looks legit.
130. Yes. I want my item.
131. Yes. I'd check to see when it would be delivered.

132. Yes. If emails is normal.
133. Yes. I would usually assume that checking the delivery progress is harmless as I am not providing them with information that they do not already have.
134. Yes. I want to know where my parcel is.
135. Yes. Yes, because I would like to know where my item is and when it's arriving.
136. Yes. To check my order.
137. Yes. Would want to know when its arriving.
138. Yes. I want to see when my item is arriving.
139. Yes. I would want to know when my parcel would be delivered.
140. Yes. Only if it looks like the company.
141. Yes. I want to make sure my parcel arrives on time.
142. Yes. I would click the link if it looked like it was real and from the company.
143. Yes. As it looks like it's from the company because of the amount of information it gives.
144. Yes. I would assume it is the confirmation.
145. Yes. I would want to check the delivery progress of the item.
146. Yes. I would open the email as this relates to my purchase.
147. Yes. Want to know where my purchase is.
148. Yes. Only if the link was clean and the email sender was correct- basically if the email looked trustworthy (no typos).
149. Yes. I want to make sure my order is going to be delivered.
150. Yes. If they have the correct order number, then I would assume it was a real email.
151. Yes. I would trust the website and want to know about the delivery.

152. Yes. Once I have checked who the email has come from. I would most likely click on the link because it is not requiring me to enter details.
153. Yes. Only if the details are extensive- includes delivery address, purchase method- and the logo exists.
154. Yes. If it was an email from the company I ordered if from I would open it.
155. No. I would not to be sure it would be a legitimate email. I have made the mistake before and the email was a virus.
156. Yes. If includes details specifically and is known.
157. Yes. To track where my parcel is.
158. Yes. To see when the item is being delivered.
159. Yes. If it looks like a legit site, and legit link/email then yes, I would.
160. Yes. If the order email was from the company I ordered from then yes.
161. Yes. I often click the link in my emails to keep updated on the delivery progress.
162. Yes. I often click on the link to check upon my delivery progress.
163. Yes. Yes, provided that the parcel has been dispatched and that the website is encrypted.
164. Yes. I trust the website.
165. Yes. I want to track my item.
166. Yes. Because I trusted the site and want to know where my parcel is.
167. Yes. Because I want to check the progress of my item.
168. Yes. To see where my parcel is.
169. Yes. I want to make sure I am at home to receive the order.
170. Yes. Yes, if the email was from a legitimate company.
171. Yes. I trust them if I ordered them.

172. Yes. I would click on the link to track my delivery.
173. Yes. I would click the link because I want to track my delivery for my item.
I trust that the link is legitimate before I click on the link.
174. Yes. Want to see where it is.
175. Yes. I like to track my delivery.
176. Yes. So I know where my package is and when it will delivered.
177. Yes. I want to find out where my parcel is.

Appendix F: Question 5 Students Response Data

Key: Open, Not Open, Check Source, Other.

1. Open the attachment.
2. Click on it.
3. Not open it.
4. If it was from an expected source, then yes.
5. Depends who it's from.
6. Make sure the attachment is from someone I expected it to come from.
7. If a spam, then I would delete.
8. I would not open it for potential viruses.
9. Depends who it I from. If I recognise it I would open it.
10. Open it.
11. Don't click on the attachment until you know it's legit.
12. I wouldn't open it unless it was from a legit website.
13. Not click it.
14. Only click if I know the sender.
15. If it was from an address, I recognised I would open it, if it wasn't, I would ignore it.
16. It depends on the sender of the email. I wouldn't open it.
17. I would click on it to see.
18. Not open unless I trust it.
19. Open it if it was familiar e.g., familiar company or person.
20. Depends what/who the email is from if I recognise the sender, I would open it.
21. Not open it and delete straight away.
22. Unless I trust the sender, leave it alone.
23. Check who the email is from and what the email says. Only open attachment if it's legitimate.
24. Open it depending on who it was from.
25. If it wasn't known, it would be deleted.

26. Unless it was from someone, I knew like a family member I would delete without opening it
27. Dependant on email. Majority of time I would ignore it.
28. Usually open it if it is expected.
29. Depends on who it is from- stranger=not open it. Someone I know=open it
30. Not click it as it seems a bit odd. I don't typically trust attachments on an email.
31. Do not click on the attachment depending on the type of email.
32. Click it.
33. Depending on the email. It looks legit then yes.
34. If I know the person who's send it I will open it if not I will delete it.
35. Most likely open it, if it shows importance.
36. I would assume it was a virus or an attempt to gain information off me and so would not click on it.
37. Depends on email.
38. Ignore it unless I thought I knew what it was in relation to i.e. not a scam.
39. Open it.
40. Open it.
41. I would check who it's from if I don't know or recognise the sender, I would delete it.
42. Depending on who it was from and if I was subscribed to something, I would open it.
43. Look at the attachment if the email is relevant.
44. Do not open link, can be a scam.
45. It would depend on the context. If I'm expecting an email with a link from a specific sender, I would open it, if not I would ignore it.

46. Depends who the email was from. Mostly, I would open the link however, if I feel like its dodgy I won't.
47. Depends on who the person who is sending the email is, if I recognise them then I might but if I don't then I won't open the link. With chain emails even if its from someone I recognise, if it looks weird, I won't open it.
48. Depends on who the person who is sending the email is, if I recognise them then I might but if I don't then I won't open the link. With chain emails even if it's from someone I recognise, if it looks weird, I won't open it.
49. If I didn't know who it was from or expect it I wouldn't open it.
50. I would not even bother to open attachments I would be suspicious.
51. Not open it unless I know the email address personally or I know I have been in contact with someone who has sent it over.
52. Maybe open it if it seems legit.
53. Email them or do a web live chat.
54. Depends what the email address was.
55. Open it if I knew it was safe (from a known email).
56. See what it is.
57. Open the attachment.
58. Wouldn't open it.
59. I would tap the email on google to see if it is not a fraud.
60. Probably wouldn't open the link if I had not heard of the sender.
61. Depending where and who the emails from open it.
62. Depends on the email.
63. It depends who I received the email from. If it was someone I knew/website I recognised, I would open it.
64. Don't open it until I've checked who sent the email.

65. Open the attachment.
66. Only people I trust.
67. If I didn't know who the email was from, I wouldn't open it.
68. It depends on who the email is from, if I don't recognise it I would not open.
69. Only if it's from a sender that I trust.
70. Don't open it if it's an unknown email address.
71. Look at the email first.
72. Wouldn't open it unless I was expecting an email of this nature.
73. If I knew the person and was expecting an email.
74. Open the attachment, only if PDF.
75. Check if I know the sender and if I was expecting the email.
76. Do not click on attachment.
77. Depending who it is from, I would open it.
78. If email looks real click on attachment.
79. If it is identifiable to me then I will open the attachment, however if looks like an unusual email, I will not open it.
80. Open it depending on who it was from.
81. Depends on the context of the email. If its relevant, then I would open it.
82. Depending on the legitimacy of the email and the name of the hyperlink would influence whether or not I click on it.
83. Leave it.
84. Look at the attachment if the email seems legit.
85. Probably open it.
86. Delete the email not open the attachment unless it was from a trusted person or company.

87. It depends who it's from. If it's from an unknown person I will most likely not open it unless there is a message explaining the attachment.
88. If it from someone I know I'd open it, if I don't know them, I'd leave it.
89. Open it if it's from an account that I recognise, unless it seems unlikely for them to send it (hacked).
90. Open it? Why wouldn't you? Unless it looked illegitimate.
91. Open it if I recognised who it was from.
92. Do not click on the attachment.
93. Depends who the email was from, but probably not open it.
94. I would open it dependent if I know who it was from if not I would ignore I delete email.
95. I would check the email, depending on who it is from I would view the attachment.
96. Depends what the email is.
97. Delete it if I recognise it to be a phishing email.
98. Depends on who it is from, if it is from a recognised or trusted source, I would open it.
99. If from an unknown account, not open it.
100. If the sender is unknown, ignore.
101. Depending on who it was from i.e., secured and trusted I would open it. If I wasn't sure I would leave it.
102. Depends who it's from... Either open or delete.
103. Open it.
104. If I didn't recognise the email address then I would delete.
105. If it was from an unknown source then I would leave it and delete it.
106. I would only open it if I knew who it was from.

107. I usually check the sender or name to see if it can be recognised or any spelling mistakes or unnecessary information is present in the email.
108. Double check the sender email address and not open the email if I'm unsure.
109. If it is from someone I don't know I would ignore it.
110. See and ensure I know who it's from before opening.
111. Unless from a trusted source I would not click.
112. Check who it's from and report it if seems dodgy.
113. Depends who it's from i.e., government.
114. I would not open the attachment until I know that the sender is not a scammer/I'd look up the sender's email.
115. Depends if it is relevant to me.
116. See who it is from and if it is 100% to click on it.
117. Always click on it if it is from a trusted address, but if it's an unknown website I'm unsure of I will google them and make a decision from there.
118. Look at who sent it and if it is someone reliable, I would open it.
119. Check who the email is from and see if it is a trusted sender, also see what the attachment is about.
120. Ignore the email.
121. Look who sent it.
122. Depends if I'm expecting an email. I wouldn't open it otherwise.
123. I wouldn't open it unless I know who it's from or I was expecting it.
124. If it's a spam email I would just delete it.
125. Unless it's clear that this is a legitimate email, I would not click it.
126. Not open it.

- 127. Nothing wouldn't open.
- 128. It depends who the email was sent by.
- 129. Be aware when opening it.
- 130. If I didn't know the sender, then not open the link and report as spam.
- 131. Depends what the email is about?
- 132. Depends on who's it's from if I didn't know them- I wouldn't open it.
- 133. Depends whether it's something important to me?
- 134. I would only open an attachment if I knew where it was from. If I wasn't sure I would ask the person it was from.
- 135. Depends on who sent the email. If I trusted it I would open.
- 136. Depending on what website, I would probably ignore it.
- 137. Yes/No. Depending on the sender.
- 138. Not open it if I do not know the sender.
- 139. Open it.
- 140. Probably open the attachment.
- 141. Never open it.
- 142. Ignore it, attachment would be a virus.
- 143. Depends who from.
- 144. Ignore it if it's something I've shouldn't be getting an email.
- 145. Open it depending on the sending.
- 146. Depending on where the email was from, I would maybe not even open the email.
- 147. Think if it is worthy of opening and if it is real thing.
- 148. Depending when I received them inbox, open and if it's in inbox I will delete if I know from who I'm getting the email or not.

149. Depends if I know the sender or was expecting an attachment. If it was from a friend I would check the validity of it first.
150. Check that I know who it is from.
151. I would not open as I would not know what I would be opening.
152. I don't usually, open them.
153. Not open it.
154. Check the email address was real.
155. Search around online to see if it's legit.
156. Open it depending on who sent it to me.
157. I wouldn't open it, unless I 100% knew what and who it's from.
158. Unless the email is from a trusted source I wouldn't open it.
159. Ignore it and delete the email.
160. If I do not know who has sent the email. I will not open the attachment.
161. Unless marked important I wouldn't open it.
162. I wouldn't open it unless I recognise the email/ if I am expecting to receive an email.
163. Don't click on it.
164. Open it if it was from a known source or sender but delete if not.
165. If it's from a source I know is trusted, then I would open them. If from unknown source I'd disregard the email.
166. Unless you know the sender/the reason the email was send don't click the attachment.
167. Generally, open it as it most likely may mean something. They can't hack me from opening an attachment.
168. It depends who it's from.

- 169. Don't look or download it.
- 170. Depends on the email and the attachment.
- 171. Open it to see what the attachments show.
- 172. Open the attachments.
- 173. Just open the attachments.
- 174. If it's from someone I don't know I wouldn't open it as I don't trust them.
But I would open it if it's from a family/friend or an official company.
- 175. Depends where it's from. If I didn't expect to get it I'd ignore/delete.
- 176. Depending on who's it's from I would either open it or ignore it.
- 177. Delete.

Appendix G: Question 6 Students Response Data

- 1. I am not sure what these terms mean.
- 2. Not giving out personal information or bank details etc
- 3. Don't open anything you are unsure about
- 4. Double check the message.
- 5. Protect my personal information. Be aware of suspicious information.
- 6. I don't know.
- 7. Block number/ Don't give out email.
- 8. Do not give number out to dodgy sites or companies or people.
- 9. I don't know.
- 10. Don't give your number out, only give my email when necessary.
- 11. Block my spam emails from my inbox.

12. Blocking some sites.
13. Do not open from unknown websites.
14. Don't open links from emails/ texts you do not know.
15. Verify the email address or the phone number and if not don't answer.
16. Block the recipient email address to save anymore emails from being sent.
17. Block the email if received a phishing email to prevent further.
18. I am not sure.
19. Only open if I trust the sender. Don't give my email/number.
20. Avoid buying things or signing up to illegitimate websites.
21. Don't give your email out to people that don't tell you they are not going to share your information.
22. Not giving out email/number to unknown sources.
23. I don't know.
24. Refrain from putting personal details (number, email etc) on websites etc.
25. Higher security measures.
26. Don't sign up for spam email or give out your details to many organisations- check if they share your info with third parties.
27. Don't open links from things you don't know.
28. Only open emails from trusted sources.
29. Delete them.
30. Don't give your number out to every company and give to third party.
31. Block the emails.
32. I would not open or respond to the emails.
33. I don't know what these terms mean.

34. Not open anything I don't know.
35. Check emails and messages before opening them.
36. Be careful which emails I open.
37. Ignore them only talk to the company if I contact them through genuine addresses/phone number.
38. Don't give out emails/numbers.
39. Do research it what to look out for and be less trusting of everything sent to you.
40. Not sure what to do.
41. Don't know.
42. Don't give out details online.
43. Always check before paying and if you are not sure don't even open them.
44. I'm not sure.
45. Not open mail by unknown emails.
46. Don't sign up to random websites.
47. Not giving personal info to company I don't trust to avoid the situation. Or just ignore them.
48. Not sure.
49. Don't know what I would do.
50. Not writing your email on websites.
51. I don't know.
52. Do not open emails/calls/text, block them?
53. Don't sign up to things online and don't click links.
54. Check the sender. Have them send to spam.
55. I don't know.

56. Block the sender or set up option to place all unusual emails in junk mail.
57. Be aware of what these would look like.
58. Always double check the company, email, texts and could phone up the company if unsure.
59. Block emails and text if this carries on then keep blocking and ignoring.
60. I don't really know what phishing means.
61. I don't know what the terms mean.
62. Never heard of any of them.
63. Don't open unknown emails/SMS.
64. Not sure.
65. I do not know.
66. Not sign up to things or put email into online sign ups.
67. Use an artificial email address.
68. Not open unknown emails or emails in spam folder.
69. Not click on unknown links.
70. Google if these links are legit.
71. Fines and imprisonment for scamming.
72. Sign up for the IPS and do not click on unverified emails.
73. Only open emails from people I know.
74. Do not open emails if they seem weird.
75. Be careful where you put your email.
76. I am not quite sure.
77. Just be careful what you open and be vigilant with what you reply to.

78. Delete them and block them.
79. Check and read before giving information.
80. Check and read before disclosing information.
81. Spam filter.
82. Not clicking on links and replying until you are certain its real.
83. Not click on attachments unless I know sender or know the content is legitimate.
84. Unsure what to do.
85. Delete your email account or send specific emails to spam.
86. Virus protection. Change email.
87. Not sure.
88. Just don't click on random links and ignore them.
89. Unsure, maybe avoid entering your email address into websites unless needed.
90. Ignore the emails and do not link on any links.
91. Put them in my junk.
92. Report any phishing emails that I had obtained.
93. Purchase a security or safeguarding program or select certain emails to be marked as spam.
94. Keep email private.
95. Don't know.
96. I have no idea what these are.
97. Be careful where you put your contact info.
98. Opt out of having email address to be sent to me.
99. Don't give out your email, phone number to random people and select no to when they ask to pass your details onto other people.
100. I have no idea what most of this is. Sorry!

101. I don't know.
102. I don't know. Never been taught or told?
103. Don't open from websites you don't know.
104. Avoid dodgy websites, block the number/emails as soon as receiving. Redirect unknown emails to junk.
105. Don't go on random sites and input personal data.
106. Avoid going on dodgy websites that could lead you to have your details taken.
107. Only open messages you know who they are from or are expecting the email.
108. Looking for unusual names and email contacts and number. Any spelling mistakes on text, have some protection on your devices. Don't give out personal information.
109. Always check with friends and family when unsure and never click on a link when you are uncertain.
110. Those kind of emails/text happen if you are not cautious on the internet.
111. Be vigilant for fraudulent emails etc. Maybe install a form of software to detect phishing emails.
112. Click the provider, spelling, what it's asking for, fonts. Report and don't click on links.
113. Block known phishing email addresses.
114. Block emails and senders/numbers.
115. Do your research on the sender. Do not pay or click on links before knowing who you are dealing with.
116. Be aware and see if they are legit.
117. Always be aware who is contacting you if unsure google them, and never give our sensitive information online unless it's a trusted website.
118. Don't open anything which could potentially be dodgy.

119. Don't give out personal information to not trusted websites and check who is sharing your data with 3rd parties.
120. Don't go on dodgy websites.
121. Just don't open, answer anything you are not expecting from a legitimate company and don't ever give out details.
122. Research links you get sent and get knowledge on what each of these are.
123. Block/report spam emails.
124. Be extra vigilant and use common sense. Block any emails/addresses that you have previously received phishing from.
125. Don't open them.
126. Don't give out email address randomly. Don't open dodgy links
127. Don't. give out personal info if unsure.
128. Google the link to see if people have had problems.
129. Keep an eye on who's sending them and not opening unknown links.
130. Don't give out your phone number to websites etc.
131. Don't give your details out to unknown websites.
132. Delete/Don't open/ignore.
133. Having spyware on the device to filter these out.
134. Do not give out email/phone number etc.
135. Don't give out details.
136. Unsubscribe from their emails.
137. Do not give your email address away.
138. Not sure.
139. Block weird email addresses, don't open things you have a bad feeling about.

- 140. Block any future phishing emails.
- 141. Read terms and conditions and not allow them to share my information.
- 142. I have a software that deals with it.
- 143. Not signing up to random sites, change passwords regularly. Keep email private.
- 144. Be more cautious.
- 145. Be aware of your orders.
- 146. Check which emails I actually open.
- 147. Don't even open the email when I got it and delete.
- 148. Don't give them if you don't know the source.
- 149. Spam filter.
- 150. Be extra careful not open things you don't know who they're from.
- 151. Don't answer and ads that you might not know and any websites that are not trusted.
- 152. Verify the number and if you are unsure contact the recipient its from.
- 153. Do not know.
- 154. Do not click etc that don't seem real.
- 155. Have a better security signature like a VPN.
- 156. Don't give out your email/phone number to websites that are not trusted.
- 157. Avoid giving out your details.
- 158. I don't understand the question.
- 159. If you don't know the number calling/texting or the place/person an email has come from don't answer.
- 160. Create a spam folder for emails.

161. Have different passwords for different accounts. Put them in spam so they only appear in junk.
162. Try not to sign up to unreliable websites.
163. Don't give email to dodgy websites and don't click links.
164. By having a spyware program installed that identify and filter out those kind of emails.
165. Don't give out email on websites, don't open unknown sources.
166. Avoid emails from senders who have no reason to be emailing you.
167. Report emails that seem phishy- also don't open attachments.
168. Set up settings to avoid any future messages from unknown people.
169. Don't know.
170. Spam filter change email received settings.
171. I am not sure.
172. Don't know what to do to be honest.
173. Delete.
174. Not sure.
175. Make a note of email addresses you know or know of and check if an email you got is from that list or not.
176. Make sure these types of emails go straight into spam or junk. And I would read properly who sent the email and the email itself.
177. Block dodgy emails.